



### **HNS Newsletter**

Issue 150 - 24.02.2003.

<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. Visit Help Net Security for the latest security news - <http://net-security.org>.

---

**QUESTION:** How Vulnerable are Your Applications and Databases?

**ANSWER:** Find out by downloading a vulnerability assessment scanner that can empower you with all of the answers.

**DOWNLOAD YOUR FREE EVALUATION VERSION** of AppDetective from:  
<http://www.appsecinc.com/helpnetsecurity>

FREE DATABASE AND APPLICATION VULNERABILITY ASSESSMENT  
EVALUATION FREE WHITE PAPERS ON DATABASE SECURITY,  
SQL INJECTION, AND WORMS

Download your **FREE EVALUATION VERSION** of AppDetective and  
INFORMATIVE WHITE PAPERS on database/application security from:  
<http://www.appsecinc.com/helpnetsecurity/>

---

#### **Table of contents:**

- 1) Security news
- 2) Vulnerabilities
- 3) Advisories
- 4) Articles
- 5) Reviews
- 6) Security world
- 7) Security software
- 8) Virus news

[ **Security news** ]

-----  
**HOW TO USE A PERSONAL DNS FOR ROOT-SERVER ATTACK ISOLATION**

Provided a couple of programmers are correct, what started out as an attempt to provide better DNS server performance on Windows machines may also be one way to reduce DNS security concerns.

>> <http://www.net-security.org/news.php?id=2021>

**EVEN SECURITY FIRMS AT RISK FOR BREAK-INS**

Security engineers at Addamark Technologies noticed that someone accessed a confidential, password-protected document on the company's Web server that contained technical product details...

>> <http://www.net-security.org/news.php?id=2023>

**UK.GOV AIMS TO DEMYSTIFY SECURITY FOR SMES**

UK online for business has launched a security section on its Web site, designed to help small business keep abreast of the latest Internet threats and how to combat them.

>> <http://www.net-security.org/news.php?id=2024>

**RICHARD CLARKE'S LEGACY OF MISCALCULATION**

The outgoing cybersecurity czar will be remembered for his steadfast belief in the danger of Internet attacks, even while genuine threats developed elsewhere.

>> <http://www.net-security.org/news.php?id=2025>

**POLICE ISSUE VIRUS WARNING**

The National Hi-Tech Crime Unit has warned firms not to become complacent about antivirus protection, despite fewer reported virus infections last year.

>> <http://www.net-security.org/news.php?id=2029>

**USERS TOUT OPEN SOURCE SECURITY**

When the right technology doesn't exist or isn't available at the right price, many large companies get creative and build their own custom systems, such as routers, firewalls or VPN gear.

>> <http://www.net-security.org/news.php?id=2030>

**CREATING YOUR OWN CA**

Become your own Certificate Authority, and sign your own - or others' - SSL certificates.

>> <http://www.net-security.org/news.php?id=2031>

**HACKER ACCESSES 5.6 MILLION CREDIT CARDS**

A hacker has gained access to as many as 5.6 million Visa and

MasterCard accounts, the two companies announced.

>> <http://www.net-security.org/news.php?id=2032>

#### SECURE MYSQL DATABASE DESIGN

This article will discuss various methods to secure databases, specifically one of the most popular freeware databases in use today, MySQL.

>> <http://www.net-security.org/news.php?id=2034>

#### CISCO EXPANDS ITS LINE OF INTRUSION-DETECTION TOOLS

Cisco Systems will announce new intrusion-protection software and firewall enhancements, including functionality designed to lower IT staffing costs by reducing false or irrelevant system intrusion alarms.

>> <http://www.net-security.org/news.php?id=2035>

#### REAL BOSS TACKLES ONLINE PIRACY

The online piracy of songs and films can be stopped but just shutting down illegal file-sharing services is not enough, says Rob Glaser, boss of Real Networks.

>> <http://www.net-security.org/news.php?id=2036>

#### RUSSIAN MAJOR CELLULAR COMPANY CLIENT DATABASE STOLEN

Russian media have caused a commotion regarding the fact that the client base of Russia's largest cellular operator has been stolen.

>> <http://www.net-security.org/news.php?id=2037>

#### INTERNET FRAUD EXPANDING, SECURITY EXPERTS WARN

Corporate computer security professionals should be aware that Internet fraud is not only growing in frequency but also expanding in scope.

>> <http://www.net-security.org/news.php?id=2038>

#### XITAMI WEB SERVER REVIEW AT UNIX REVIEW

Xitami highlights a Web-based administrator, the LRWP Protocol, XML, a built-in FTP server, and more. The commercial version, Xitami Pro, supports full SSL layer 2 and 3, and uses OpenSSL source.

>> <http://www.net-security.org/news.php?id=2039>

#### MITSUBISHI DEVELOPS ONE-TIME PASSWORD SYSTEM

Engineers at Mitsubishi have developed a one-time password system for use on mobile Internet services.

>> <http://www.net-security.org/news.php?id=2040>

#### REMOTE USERS ARE THE WEAKEST LINK

Say there's a remote worker who connects to the corporate net

through a VPN, and to the Internet via broadband and a Wi-Fi hub. That broadband link could be vulnerable and let someone "piggyback" into the VPN.

>> <http://www.net-security.org/news.php?id=2042>

#### FIGHTING PIRACY WITH P2P BLOCKING

For months, the digital equivalent of a postal censor has been sorting through virtually all file-swapping traffic on the University of Wyoming's network.

>> <http://www.net-security.org/news.php?id=2044>

#### ROOT OF MASSIVE CREDIT CARD THEFT FOUND

An attacker who gained access to millions of credit card numbers did it by breaking into a computer system at a company that handles transactions for catalog companies and other direct marketers.

>> <http://www.net-security.org/news.php?id=2045>

#### SECURITY: FIGHTING THE ENEMY WITHIN

How do you protect your network against a threat you can't see? New security automation can establish policies, and consistently audit and monitor them for compliance.

>> <http://www.net-security.org/news.php?id=2046>

#### DMCA BLOCKS TECH PROGRESS

Silicon Valley executives and other insiders meet with lawmakers to discuss how the Digital Millennium Copyright Act adversely impacts technology innovation - and what they can do about it.

>> <http://www.net-security.org/news.php?id=2047>

#### HOW TO GET AN ATM PIN NUMBER IN 15 GUESSES

Cambridge researchers have documented a worrying PIN cracking technique against the hardware security modules commonly used by bank ATM machines.

>> <http://www.net-security.org/news.php?id=2050>

#### LAWYERS: HACKERS SENTENCED TOO HARSHLY

A new paper argues that hacking cases should be treated as white-collar fraud, not as terrorism.

>> <http://www.net-security.org/news.php?id=2051>

#### A USER'S GUIDE TO ONLINE SECURITY

Computer security used to mean making sure that the door was locked on your way out of the house. Thanks to the internet, security means protecting your computer from electronic assailants as well.

>> <http://www.net-security.org/news.php?id=2052>

#### SECURE CHAT WITH YTALK AND SSH

Robert Bernier re-introduces the venerable and powerful YTalk and demonstrates how it can be used securely with SSH.

>> <http://www.net-security.org/news.php?id=2053>

#### SWISS CRACK EMAIL ENCRYPTION

Researchers have found a way to unlock SSL-encrypted emails, but the real-world impact of their accomplishment is doubtful.

>> <http://www.net-security.org/news.php?id=2054>

-----

#### [ Vulnerabilities ]

All vulnerabilities are located here:

[http://www.net-security.org/archive\\_vuln.php](http://www.net-security.org/archive_vuln.php)

-----

Perl2Exe EXEs Can be Decompiled

>> <http://www.net-security.org/vuln.php?id=2464>

Symantec Norton AntiVirus 2002 Buffer Overflow Vulnerability

>> <http://www.net-security.org/vuln.php?id=2463>

Sage Cross Site Scripting and Path Disclosure Vulnerabilities

>> <http://www.net-security.org/vuln.php?id=2462>

myphpnuke Cross Site Scripting Vulnerability

>> <http://www.net-security.org/vuln.php?id=2461>

Cpanel 5 Remote Command Execution and Local Root Vulnerabilities

>> <http://www.net-security.org/vuln.php?id=2460>

Netcharts XBRL Server v4.0.0 Information Leakage Vulnerability

>> <http://www.net-security.org/vuln.php?id=2459>

D-Forum Include File Vulnerability

>> <http://www.net-security.org/vuln.php?id=2458>

php-Board Information Disclosure Vulnerability

>> <http://www.net-security.org/vuln.php?id=2457>

Kietu Include File Vulnerability

>> <http://www.net-security.org/vuln.php?id=2456>

DotBr Multiple Vulnerabilities

>> <http://www.net-security.org/vuln.php?id=2454>

Oracle9i Application Server Format String Vulnerability

>> <http://www.net-security.org/vuln.php?id=2453>

ORACLE bfilename Function Buffer Overflow Vulnerability

>> <http://www.net-security.org/vuln.php?id=2452>

Lotus iNotes Client ActiveX Control Buffer Overrun Vulnerability

>> <http://www.net-security.org/vuln.php?id=2451>

Lotus Domino Web Server Host/Location Buffer Overflow Vulnerability

>> <http://www.net-security.org/vuln.php?id=2450>

Lotus Domino Web Server iNotes Overflow Vulnerability

>> <http://www.net-security.org/vuln.php?id=2449>

Oracle TZ\_OFFSET Remote System Buffer Overrun Vulnerability

>> <http://www.net-security.org/vuln.php?id=2448>

Oracle TO\_TIMESTAMP\_TZ Remote System Buffer Overrun Vulnerability

>> <http://www.net-security.org/vuln.php?id=2447>

Oracle Unauthenticated Remote System Compromise

>> <http://www.net-security.org/vuln.php?id=2446>

BisonFTP Multiple Vulnerabilities

>> <http://www.net-security.org/vuln.php?id=2445>

Microsoft Windows riched20.dll attribute label buffer  
overflow vulnerability

>> <http://www.net-security.org/vuln.php?id=2444>

MacOS X TruBlueEnvironment Privilege Escalation Attack

>> <http://www.net-security.org/vuln.php?id=2443>

-----

[ **Advisories** ]

All advisories are located at:

[http://www.net-security.org/archive\\_advi.php](http://www.net-security.org/archive_advi.php)

-----  
Cisco Security Advisory: Multiple Product Vulnerabilities  
found by PROTOS SIP Test Suite  
>> <http://www.net-security.org/advisory.php?id=1628>

Mandrake Linux Security Advisory - krb5  
>> <http://www.net-security.org/advisory.php?id=1627>

Mandrake Linux Security Advisory - openssl  
>> <http://www.net-security.org/advisory.php?id=1626>

Trustix Security Advisory - openssl  
>> <http://www.net-security.org/advisory.php?id=1625>

CERT Advisory CA-2003-06 - Multiple vulnerabilities in  
implementations of the Session Initiation Protocol (SIP)  
>> <http://www.net-security.org/advisory.php?id=1624>

Debian Security Advisory - New slocate packages fix  
local root exploit  
>> <http://www.net-security.org/advisory.php?id=1623>

Conectiva Linux Security Announcement - kde  
>> <http://www.net-security.org/advisory.php?id=1622>

Compaq Security Bulletin - HP Tru64 UNIX, HP-UX,  
Potential BIND Security Vulnerabilities  
>> <http://www.net-security.org/advisory.php?id=1621>

Red Hat Security Advisory - Updated shadow-utils  
packages fix exposure  
>> <http://www.net-security.org/advisory.php?id=1620>

Gentoo Linux Security Announcement - bitchx  
>> <http://www.net-security.org/advisory.php?id=1619>

Gentoo Linux Security Announcement - openssl  
>> <http://www.net-security.org/advisory.php?id=1618>

EnGarde Secure Linux Advisory - OpenSSL timing-based  
attack vulnerability  
>> <http://www.net-security.org/advisory.php?id=1617>

EnGarde Secure Linux Advisory - MySQL double free vulnerability  
>> <http://www.net-security.org/advisory.php?id=1616>

Mandrake Linux Security Advisory - php  
>> <http://www.net-security.org/advisory.php?id=1615>

CERT Advisory CA-2003-05 - Multiple Vulnerabilities  
in Oracle Servers  
>> <http://www.net-security.org/advisory.php?id=1614>

EnGarde Secure Linux Advisory - Several PHP vulnerabilities  
>> <http://www.net-security.org/advisory.php?id=1613>

OpenPKG Security Advisory - openssl  
>> <http://www.net-security.org/advisory.php?id=1612>

OpenPKG Security Advisory - dhcpcd  
>> <http://www.net-security.org/advisory.php?id=1611>

Gentoo Linux Security Announcement - mod\_php  
>> <http://www.net-security.org/advisory.php?id=1610>

Gentoo Linux Security Announcement - mod\_php php  
>> <http://www.net-security.org/advisory.php?id=1609>

PHP Security Advisory - CGI vulnerability in PHP version 4.3.0  
>> <http://www.net-security.org/advisory.php?id=1608>

Mandrake Linux Security Advisory - apcupsd  
>> <http://www.net-security.org/advisory.php?id=1607>

Mandrake Linux Security Advisory - pam  
>> <http://www.net-security.org/advisory.php?id=1606>

SuSE Security Announcement - mod\_php4  
>> <http://www.net-security.org/advisory.php?id=1605>

SuSE Security Announcement - imp  
>> <http://www.net-security.org/advisory.php?id=1604>

OpenPKG Security Advisory - lynx  
>> <http://www.net-security.org/advisory.php?id=1603>

OpenPKG Security Advisory - php, apache  
>> <http://www.net-security.org/advisory.php?id=1602>

OpenPKG Security Advisory - w3m  
>> <http://www.net-security.org/advisory.php?id=1601>

Gentoo Linux Security Announcement - nethack  
>> <http://www.net-security.org/advisory.php?id=1600>

Gentoo Linux Security Announcement - w3m  
>> <http://www.net-security.org/advisory.php?id=1599>

Gentoo Linux Security Announcement - syslinux  
>> <http://www.net-security.org/advisory.php?id=1598>

Gentoo Linux Security Announcement - mailman  
>> <http://www.net-security.org/advisory.php?id=1597>

SCO Security Advisory - Linux: Apache mod\_dav module  
format string vulnerability  
>> <http://www.net-security.org/advisory.php?id=1596>

Debian Security Advisory - New CUPS packages fix wrong  
libPNG dependency  
>> <http://www.net-security.org/advisory.php?id=1595>

SGI Security Advisory - IP denial-of-service fixes  
and tunings  
>> <http://www.net-security.org/advisory.php?id=1594>

-----

**[ Featured 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 [staff@net-security.org](mailto:staff@net-security.org)

---

**INTERVIEW WITH ED SKOUDIS, AUTHOR OF "COUNTER HACK"**

Ed Skoudis is the Vice President of Security Strategy for Predictive Systems. Ed's expertise includes hacker attacks and defenses, the information security industry, and computer privacy issues.

>> <http://www.net-security.org/article.php?id=391>

**INTERVIEW WITH JUDY NOVAK, CO-AUTHOR OF "NETWORK INTRUSION DETECTION 3/E"**

Read her opinion on intrusion detection, open source, the disclosure of vulnerabilities and more.

>> <http://www.net-security.org/article.php?id=393>

**TRUSTIX SECURE LINUX 2.0 TECHNOLOGY PREVIEW 2 RELEASED**

Trustix team announced that Trustix Secure Linux 2.0 Technology Preview 2 (aka Forecast) is available for download.

>> <http://www.net-security.org/article.php?id=392>

**NEW OPENSLL SECURITY AND BUGFIX RELEASES**

The OpenSSL announced the release of version 0.9.7a of their open source toolkit for SSL/TLS.

>> <http://www.net-security.org/article.php?id=394>

**FIRST HONEYD CHALLENGE - TEST YOUR PROGRAMMING SKILLS**

Honeyd is a virtual honeypot running as a small daemon to create virtual hosts on a network. The hosts can be configured to run arbitrary services and their personality can be adapted so that they appear to be running certain operating systems.

>> <http://www.net-security.org/article.php?id=395>

---

[ **Reviews** ]

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

-----  
**CISCO SECURE VIRTUAL PRIVATE NETWORKS**  
This publication is designed to give the readers basic knowledge of planning, administering and maintaining Virtual Private Networks. It does provide some general VPN related information, but as it is a written reference for the Cisco Secure Virtual Private Networks courses, book will be of a great use to the readers wanting to enable VPN with their Cisco products.  
>> <http://www.net-security.org/review.php?id=33>

**MISSION-CRITICAL SECURITY PLANNER: WHEN HACKERS WON'T TAKE NO FOR AN ANSWER**  
If you want to do security planning and you don't know where to start, this book is mandatory reading material. It will make your life easier and your system more secure.  
>> <http://www.net-security.org/review.php?id=34>

[ **Security world** ]

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

-----  
**Datakey introduces Datakey Axis – A Solution for Simplified Access and Identity Management**  
>> <http://www.net-security.org/press.php?id=1258>

**Phoenix Technologies Unveils cME; Redefines Core System Solutions Built into Current and Next-Generation PCs and Digital Products**  
>> <http://www.net-security.org/press.php?id=1257>

**GFI Releases GFI MailEssentials for Exchange/SMTP 8**  
>> <http://www.net-security.org/press.php?id=1256>

Lindows.com Introduces Built-in Antivirus Defense System  
for LindowsOS

>> <http://www.net-security.org/press.php?id=1255>

Port80 Software and Federal Systems Group Announce Distribution  
& Consulting Partnership Focused on Web Server Anonymization  
for Enhanced Network Security

>> <http://www.net-security.org/press.php?id=1254>

F-Secure Unveils the World's First Content Security Solution  
for Wireless Download Systems

>> <http://www.net-security.org/press.php?id=1253>

Remote Update From Sophos Streamlines Anti-Virus Protection  
For Remote Workers

>> <http://www.net-security.org/press.php?id=1252>

SSH Enables Secure Remote Management Of Network Devices  
With SSH Secure Shell Toolkit 4.0

>> <http://www.net-security.org/press.php?id=1251>

SSH Unveils New Toolkit For Securing Web-Based Remote  
Management Of Network Devices

>> <http://www.net-security.org/press.php?id=1250>

F-Secure to Provide Security Solutions for the Sony  
Ericsson P800 Smart Phone

>> <http://www.net-security.org/press.php?id=1249>

ZNQ3 Names Billman as Vice President, Engineering & Development

>> <http://www.net-security.org/press.php?id=1248>

ZNQ3 Names Platt as Chief Operating Officer

>> <http://www.net-security.org/press.php?id=1247>

New CryptoHeaven Packages For Small Business

>> <http://www.net-security.org/press.php?id=1246>

Endeavors Technology Releases Advanced Instant Conferencing  
Tools for Business Critical Decision Teams Using WebEx Meetings

>> <http://www.net-security.org/press.php?id=1245>

Intrusion Inc. Gigabit IDS Awarded Miercom NetWORKS  
As Advertised Award

>> <http://www.net-security.org/press.php?id=1243>

Sygate Outperforms Symantec In Independent Test  
Of Enterprise Security Solutions  
>> <http://www.net-security.org/press.php?id=1243>

---

[ **Security 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)

---

QUICKTABLES 1.1 (Linux)  
Quicktables is an iptables firewall and firewall/NAT (gateway) script generator. It was created to provide a secure set of iptables rules quickly.  
>> <http://www.net-security.org/software.php?id=453>

LABREA HONEYPOT 2.4 (Windows)  
LaBrea takes over unused IP addresses, and creates virtual servers that are attractive to worms, hackers, and other denizens of the Internet.  
>> <http://www.net-security.org/software.php?id=454>

SNORTALOG 1.7.0 (Linux)  
Snortalog is a powerfull perl script that summarize snort logs making an easy view of what attacks are being seen through your network.  
>> <http://www.net-security.org/software.php?id=455>

CHANGE PASSWORD UTILITY 1.3.99 (Linux)  
CPU is an LDAP user management tool written in C and loosely based on FreeBSD's pw(8). The goal of CPU is to be a suitable replacement of the useradd/usermod/userdel utilities for administrators using an LDAP backend and wishing to have a suite of command line tools for doing the administration.  
>> <http://www.net-security.org/software.php?id=456>

---

[ **Virus News** ]

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

-----  
Lovgate, Tang and Kingpdt Worms, Nzlog and Aileen Trojans  
>> [http://www.net-security.org/virus\\_news.php?id=188](http://www.net-security.org/virus_news.php?id=188)

Kazoa Worm, NTRootkit Tool and Egruf Trojan  
>> [http://www.net-security.org/virus\\_news.php?id=187](http://www.net-security.org/virus_news.php?id=187)

-----  
Questions, contributions, comments or ideas go to:

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

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

Unsubscribe by sending your e-mail address to:  
info@net-security.org with UNSUBSCRIBE in the message body.

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)

-----  
QUESTION: How Vulnerable are Your Applications and Databases?

ANSWER: Find out by downloading a vulnerability assessment scanner that can empower you with all of the answers.

**DOWNLOAD YOUR FREE EVALUATION VERSION** of AppDetective from:  
<http://www.appsecinc.com/helpnetsecurity>

FREE DATABASE AND APPLICATION VULNERABILITY ASSESSMENT  
EVALUATION FREE WHITE PAPERS ON DATABASE SECURITY,  
SQL INJECTION, AND WORMS

Download your **FREE EVALUATION VERSION** of AppDetective and  
INFORMATIVE WHITE PAPERS on database/application security from:  
<http://www.appsecinc.com/helpnetsecurity/>

-----