



Newsletter
Issue 133

Issue 133 - 28.10.2002

<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>.

HELP NET SECURITY 4TH ANNIVERSARY

Today HNS celebrates it's 4th year of online presence. We would like to thank all the visitors and contributors that helped us become what we are today.

Want some knowledge? We're giving away 3 copies of "Internet Site Security": <http://www.net-security.org/news.php?id=1327>

Table of contents:

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

[General security news]

CHROOTING DAEMONS AND SYSTEM PROCESSES HOW-TO

The purpose of chrooting is designed to create an impenetrable (theoretically) "jail" protecting what is being chrooted from being able to read or modify any files outside of the chrooted environment.
>> <http://www.net-security.org/news.php?id=1275>

PC SECURITY: SUITE YOURSELF

Surfing the Net without some level of security has become like driving in NASCAR without a seat belt.
>> <http://www.net-security.org/news.php?id=1276>

MIT PALLADIUM PRESENTATION

Last friday Brian LaMacchia from Microsoft held a presentation about a set of hardware and software security features currently under development for a future version of the Windows operating system.
>> <http://www.net-security.org/news.php?id=1278>

SA SITES HIT BY HACKER

A hacker is reported to have targeted at least 20 South African Web sites last week, 14 of the attacks occurring in a single day.

>> <http://www.net-security.org/news.php?id=1279>

KEEP UNWANTED GUESTS OFF YOUR WIRELESS NET

Your Wi-Fi network could be an open door to attackers. Here's how to close it.

>> <http://www.net-security.org/news.php?id=1281>

FEDS WARMING TO THE IDEA OF REGULATING SECURITY

White house security officials are coming around to the idea that government regulation of the software industry may be needed to make the National Strategy to Secure Cyberspace work.

>> <http://www.net-security.org/news.php?id=1285>

NAVY SEARCHING FOR HUNDREDS OF MISSING COMPUTERS

At least 595 laptops and desktops belonging to the Navy's Pacific Command in Hawaii have been potentially lost or compromised, according to an internal report.

>> <http://www.net-security.org/news.php?id=1286>

THE RISE OF ENCRYPTION

Over the past three years, sales of encryption products have jumped 86%, to \$248 million - a figure that will rise to \$379 million by 2006, according to the research firm IDC.

>> <http://www.net-security.org/news.php?id=1287>

DIRECT MARKETERS ENDORSE ANTI-SPAM LAWS

The Direct Marketing Association said that unsolicited e-mail has become so noxious that a federal anti-spam law is necessary.

>> <http://www.net-security.org/news.php?id=1288>

WEB VANDALISM ON THE RISE

Web vandalism is on the rise around the world, underscoring the shoddy state of affairs in IT security, according to Zone-H.org.

>> <http://www.net-security.org/news.php?id=1289>

WHY WEB APPLICATION SECURITY IS THE NEW THREAT

The main causes of today's web application vulnerabilities lie within the development structure process. Developers are under pressure to meet deadlines and make sure the application works from day one.

>> <http://www.net-security.org/news.php?id=1290>

COMMON SECURITY MISTAKES STILL HAUNT ENTERPRISES

As enterprises expose their perimeters to customers and business partners more and more, there is less room or tolerance for security lapses.

>> <http://www.net-security.org/news.php?id=1291>

TRACKING DOWN INSECURE WLANS

Looking for something to do this weekend? Well, if you have a laptop and a wireless card, you can join dozens of other technophiles with time on their hands in searching out insecure WLANS.

>> <http://www.net-security.org/news.php?id=1295>

FIREWALLS OF THE FUTURE

As security threats facing high-speed networks grow by the day, products such as firewalls are under constant demand to become more sophisticated.

>> <http://www.net-security.org/news.php?id=1296>

SOFTWARE SECURITY - A MATTER OF TRUST

You can make a good argument that any practical computer security arrangement involves some level of trust between software providers and software users.

>> <http://www.net-security.org/news.php?id=1297>

FEDS INVESTIGATING 'LARGEST EVER' INTERNET ATTACK

US Federal authorities are investigating an attack on the internet that has been described as the "largest and most complex" in history.

>> <http://www.net-security.org/news.php?id=1298>

CALL FOR PAPERS ANNOUNCEMENT: BLACK HAT WINDOWS SECURITY

Papers and presentations are now being accepted for The Black Hat Briefings: Windows Security 2003 event in Seattle, Washington, February 26th to the 27th.

>> <http://www.net-security.org/news.php?id=1299>

WANG HACK FAQ

These FAQs explain in great detail the most common questions asked about computers and security today.

>> <http://www.net-security.org/news.php?id=1302>

EXPERTS MEET TO COMBAT CHILD PORN

An international conference of police and criminologists aims to fight the rising tide of Web-based child pornography.

>> <http://www.net-security.org/news.php?id=1304>

IMAGES GET DISTORTION-PROOF CRYPTO MARKS

Researchers from Xerox and the University of Rochester have created a new way to encrypt information in a digital image and extract it later without any distortion or loss of information.

>> <http://www.net-security.org/news.php?id=1305>

BUILDING A BETTER VIRUS DEFENSE

Antivirus on the desktop is fairly mature. However, the IT organization must now coordinate a layered defense to prevent viruses from penetrating the core network, particularly via e-mail.

>> <http://www.net-security.org/news.php?id=1306>

USING GNUPG

This article is intended as a simple introductory guide to GnuPG and not as a comprehensive guide to public key encryption.

>> <http://www.net-security.org/news.php?id=1307>

NO EASY MONEY SUING SPAMMERS

Think deleting junk e-mail is a pain? Try taking a spammer to court. Some activists are making money pursuing spam cases in small claims court, but few say the profits are worth the hassle.

>> <http://www.net-security.org/news.php?id=1308>

NET ATTACKS: INTERNET PIONEER PREDICTED OUTAGES IN 2000

Monday's attacks on the 13 root servers that serve the Internet were discussed as a distinct possibility by an Internet pioneer in The Age over two years ago.

>> <http://www.net-security.org/news.php?id=1309>

REVERSE ENGINEERING HOSTILE CODE

This article outlines the process of reverse engineering hostile code. By "hostile code", we mean any process running on a system that is not authorized by the system administrator.

>> <http://www.net-security.org/news.php?id=1310>

ARE WE LIVING IN THE GOLDEN AGE OF HACKING?

Recent months have seen an increase in security holes and in new tools used to exploit them, expert warns.

>> <http://www.net-security.org/news.php?id=1316>

WHY HACKERS DON'T CARE ABOUT WI-FI

Experts at war driving exchange location secrets and sniffing tips over the Web, the way gamers trade strategies for reaching new levels.

>> <http://www.net-security.org/news.php?id=1317>

CLOSING SPYWARE LOOPHOLES

A recent court decision against AOL Netscape finally puts some limits on the clickwrap contracts that make spyware legal.

>> <http://www.net-security.org/news.php?id=1318>

CERTIFIABLY CERTIFIED

Despite impressive acronyms that look great on a resume, security certifications don't guarantee that the holder is qualified to secure vital information.

>> <http://www.net-security.org/news.php?id=1319>

HACKER RUNS UP \$10,000 PHONE BILL

Thousands of junk e-mails charged to a Napier firm by a computer hacker are a costly lesson in company security, says a police information technology expert.

>> <http://www.net-security.org/news.php?id=1320>

[Vulnerabilities]

All vulnerabilities are located here:

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

SolarWinds TFTP Server Directory Traversal Vulnerability

>> <http://www.net-security.org/vuln.php?id=2170>

IBM Infoprint Remote Management Denial of Service Vulnerability

>> <http://www.net-security.org/vuln.php?id=2169>

Norton Antivirus Corporate Edition Privilege Escalation Vulnerability

>> <http://www.net-security.org/vuln.php?id=2168>

vpopmail CGIApps Insufficient Input Checking Vulnerability

>> <http://www.net-security.org/vuln.php?id=2167>

IBM WebSphere Edge Server Caching Proxy Cross-Site Scripting Issues

>> <http://www.net-security.org/vuln.php?id=2166>

IBM WebSphere Edge Server Caching Proxy Denial of Service

>> <http://www.net-security.org/vuln.php?id=2165>

Web Server 4 Everyone v1.28 Host Field Denial of Service Vulnerability

>> <http://www.net-security.org/vuln.php?id=2164>

FlashFXP 1.4 Local Password Disclosure Vulnerability

>> <http://www.net-security.org/vuln.php?id=2163>

gBook Administrator Access Vulnerability

>> <http://www.net-security.org/vuln.php?id=2162>

phpnewsDev "include" Vulnerability

>> <http://www.net-security.org/vuln.php?id=2161>

Virgil CGI Scanner 0.9 Privilege Escalation Vulnerability

>> <http://www.net-security.org/vuln.php?id=2160>

Internet Explorer Vulnerable Cached Objects

>> <http://www.net-security.org/vuln.php?id=2159>

Sniffing Administrator's Password in Symantec
Firewall/VPN Appliance
>> <http://www.net-security.org/vuln.php?id=2158>

D-Link Access Point DWL-900AP+ TFTP Vulnerability
>> <http://www.net-security.org/vuln.php?id=2157>

Pafilledb Cross Site Scripting Vulnerability
>> <http://www.net-security.org/vuln.php?id=2156>

RPC Service Denial of Service on Windows 2000 SP3
>> <http://www.net-security.org/vuln.php?id=2155>

vBulletin Cross Site Scripting Vulnerability
>> <http://www.net-security.org/vuln.php?id=2154>

Web602 Web Server Multiple Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=2153>

perlbot 1.0 beta Remote Command Execution
>> <http://www.net-security.org/vuln.php?id=2152>

[Advisories]

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

NetBSD Security Advisory - trek(6) buffer overrun
>> <http://www.net-security.org/advisory.php?id=1194>

Mandrake Linux Security Advisory - mod_ssl
>> <http://www.net-security.org/advisory.php?id=1193>

Mandrake Linux Security Advisory - kdegraphics
>> <http://www.net-security.org/advisory.php?id=1192>

Gentoo Linux Security Announcement - zope
>> <http://www.net-security.org/advisory.php?id=1191>

SCO Security Advisory - Linux: various packet handling vulnerabilities in ethereal
>> <http://www.net-security.org/advisory.php?id=1190>

Gentoo Linux Security Announcement - xfree
>> <http://www.net-security.org/advisory.php?id=1189>

Red Hat Security Advisory - Updated ypserv packages fixes memory leak
>> <http://www.net-security.org/advisory.php?id=1188>

Mandrake Linux Security Advisory - tetex
>> <http://www.net-security.org/advisory.php?id=1187>

OpenPKG Security Advisory - apache
>> <http://www.net-security.org/advisory.php?id=1186>

SCO Security Advisory - Linux: remote buffer overflow in webalizer reverse lookup code
>> <http://www.net-security.org/advisory.php?id=1185>

Debian Security Advisory - New mod_ssl packages fix cross site scripting
>> <http://www.net-security.org/advisory.php?id=1184>

EnGarde Secure Linux Advisory - local kernel vulnerabilities
>> <http://www.net-security.org/advisory.php?id=1183>

NetBSD Security Advisory - Insufficient length check in ESP authentication data
>> <http://www.net-security.org/advisory.php?id=1182>

NetBSD Security Advisory - Buffer overflow in kadmind daemon
>> <http://www.net-security.org/advisory.php?id=1181>

Mandrake Linux Security Advisory - gv/ggv
>> <http://www.net-security.org/advisory.php?id=1180>

SCO Security Advisory - UnixWare 7.1.1 Open UNIX 8.0.0: rcp of /proc causes denial-of-service
>> <http://www.net-security.org/advisory.php?id=1179>

SuSE Security Announcement - postgresql
>> <http://www.net-security.org/advisory.php?id=1178>

Debian Security Advisory - New NIS packages fix information leak
>> <http://www.net-security.org/advisory.php?id=1177>

Debian Security Advisory - New gnome-gv packages fix buffer overflow

>> <http://www.net-security.org/advisory.php?id=1176>

Gentoo Linux Security Announcement - groff

>> <http://www.net-security.org/advisory.php?id=1175>

Gentoo Linux Security Announcement - tetex

>> <http://www.net-security.org/advisory.php?id=1174>

Red Hat Security Advisory - Updated Mozilla packages fix security vulnerabilities

>> <http://www.net-security.org/advisory.php?id=1173>

[Featured articles]

All articles are located at:

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

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

ICSA LABS ANNOUNCES Q3 2002 CERTIFICATIONS
ICSA Labs, an independent division of TruSecure Corporation announced that it has certified sixteen products in Q3 2002.
>> <http://www.net-security.org/article.php?id=213>

DBCC SHOWTABLEAFFINITY BUFFER OVERRUN
Martin Rakhmanoff wrote this article to (better) document the process of finding and exploiting buffer overrun bugs.
>> <http://www.net-security.org/article.php?id=214>

CAN YOU TRUST YOUR COMPUTER?
Who should your computer take its orders from? Most people think their computers should obey them, not obey someone else. With a plan they call "trusted computing," large media corporations (including the movie companies and record companies), together with computer companies such as Microsoft and Intel, are planning to make your computer obey them instead of you.
>> <http://www.net-security.org/article.php?id=215>

OPEN SOURCE DIGITAL FORENSICS TOOLS: THE LEGAL ARGUMENT
This paper addresses digital forensic analysis tools and their use in a legal setting.
>> <http://www.net-security.org/article.php?id=216>

CHECK POINT EXPANDS SECURITY MANAGEMENT ARCHITECTURE PRODUCT LINE

Check Point Software Technologies, one of the key players in the VPN and firewall markets, announced two add-ons to their SMART (Security Management Architecture) product line - SmartView Reporter and SmartView Monitor.

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

THE NORMAN BOOK ON COMPUTER VIRUSES

One of the most high-profile threats to information integrity is the computer virus. Surprisingly, PC viruses have been around for two-thirds of the IBM PC's lifetime, appearing in 1986. With global computing on the rise, computer viruses have had more visibility in the past two years.

>> <http://www.net-security.org/article.php?id=218>

RSA SECURITY COLLABORATES WITH AMD TO BOOST SECURITY

RSA Security Inc. announced they are collaborating with Advanced Micro Devices to deliver optimized encryption software for current AMD Athlon processors and upcoming AMD processors based on Hammer technology.

>> <http://www.net-security.org/article.php?id=219>

THE COMPLETE WINDOWS TROJANS PAPER

This is a paper about Windows Trojans, how they work, their variations and, of course, strategies to minimise the risk of infection.

>> <http://www.net-security.org/article.php?id=220>

DEALING WITH EXTERNAL COMPUTER SECURITY INCIDENTS

Dealing with computer security incidents is extremely difficult. There are many ways that incidents can occur and many types of impact they can have on an organization.

>> <http://www.net-security.org/article.php?id=221>

COUNTERING CYBER WAR

Timothy Shimeall, Phil Williams and Casey Dunlevy argue that defence planning has to incorporate the virtual world to limit physical damage in the real.

>> <http://www.net-security.org/article.php?id=222>

MCAfee ANTI VIRUS INCLUDED ON MSN 8 CD-ROM

McAfee Security Consumer announced a partnership with MSN. According to the terms, McAfee VirusScan Online will be included in the MSN 8 cd-rom.

>> <http://www.net-security.org/article.php?id=223>

[Security world]

All press releases are located at:
http://www.net-security.org/press_main.php

Ferrari UK accelerates to lower IT costs with IBM and
Trustix Linux Solutions

>> <http://www.net-security.org/press.php?id=1077>

RAV AntiVirus for File Servers (Win32) - a Silken Shield
With Steel Toughness

>> <http://www.net-security.org/press.php?id=1076>

ActiveState's PerlMx Offers Integrated Anti-Spam Solution
with McAfee Security Anti-Virus Protection

>> <http://www.net-security.org/press.php?id=1075>

netForensics Unveils the Next Generation of Security
Information Management

>> <http://www.net-security.org/press.php?id=1074>

F-Secure Receives World's First Security Certificate
For Windows Powered Mobile Platforms

>> <http://www.net-security.org/press.php?id=1073>

Cyberguard Firewalls To Protect Major Mideast Telecom

>> <http://www.net-security.org/press.php?id=1072>

Datakey Announces Third Quarter Results

>> <http://www.net-security.org/press.php?id=1071>

Cisco Systems to Acquire Psionic Software

>> <http://www.net-security.org/press.php?id=1070>

Baltimore Is First To Remove The Cost and Complexity
of PKI Security

>> <http://www.net-security.org/press.php?id=1069>

Snapgear Launches Into Controller Market

>> <http://www.net-security.org/press.php?id=1068>

[Security 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

EASY FIREWALL GENERATOR 1.07

Easy Firewall Generator is a PHP Web application that generates an iptables firewall script.

>> <http://www.net-security.org/software.php?id=325>

IPKUNGFU 0.1.1

IPKungFu is a script aiming to simplify the configuration of your firewall/NAT/port forwarding. It takes advantage of advanced features of iptables and tcpwrappers.

>> <http://www.net-security.org/software.php?id=326>

JAMMER 2.0

Jammer's efficient detection mechanisms locate and block every type of Trojan, Backdoor, Adware and Spyware.

>> <http://www.net-security.org/software.php?id=327>

BUBBLEGUM 1.12

Bubblegum is a small daemon written in C which watches a files access, modification and inode change times and MD5 checksums.

>> <http://www.net-security.org/software.php?id=328>

GFI MAILESENTIALS FOR EXCHANGE/SMTP 7.1

GFI MailEssentials for Exchange/SMTP is a server based anti Spam & email management solution for Microsoft Exchange Server, Lotus Notes and SMTP/POP3 mail servers.

>> <http://www.net-security.org/software.php?id=329>

CRYPTOMITE 1.53

CryptoMite is a fast and very easy-to-use program which is able to lock and block access to files of every type and even whole directory structures. For this it uses strong encryption, encryption acknowledged worldwide to be unbreakable.

>> <http://www.net-security.org/software.php?id=330>

INTEGRIT 3.02.00

Integrit is an alternative to file integrity verification programs like tripwire and aide. It helps you determine whether an intruder has modified a computer system.

>> <http://www.net-security.org/software.php?id=331>

ZONELOG ANALYSER 1.15

ZoneLog Analyser reads and displays the log file generated by ZoneLabs' ZoneAlarm and ZoneAlarm Pro (V2.1.10 and later) personal firewall, entries in the log are generated whenever an unauthorised connection is attempted to or from your PC during connection to the Internet.

>> <http://www.net-security.org/software.php?id=332>

HPING 2.0.0-RC1

hping is a command-line oriented TCP/IP packet assembler/analyzer.

>> <http://www.net-security.org/software.php?id=333>

VPND 1.1.0

The virtual private network daemon vpnd is a daemon which connects two networks on network level either via TCP/IP or a (virtual) leased line attached to a serial interface. All data transferred between the two networks are encrypted using the unpatented free Blowfish encryption algorithm.

>> <http://www.net-security.org/software.php?id=334>

[Virus News]

All virus news are located at:

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

RAV AntiVirus for File Servers (Win32) Released

>> http://www.net-security.org/virus_news.php?id=107

Opaserv.F and Opaserv.G Worms Detected

>> http://www.net-security.org/virus_news.php?id=106

Panda Software Reports on New Opaserv.E Worm

>> http://www.net-security.org/virus_news.php?id=105

Panda Software Weekly Virus Report

>> http://www.net-security.org/virus_news.php?id=104

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