



Newsletter
Issue 139

Issue 139 - 09.12.2002

<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>.

SECURITY INCIDENT ALERT

Check your Web servers, FTP servers, Mail servers , DNS servers, firewalls, IDS systems, switchers and routers for over 900 up to date vulnerabilities. Secure your critical assets today!

FREE System Security Test and Detailed Report
<http://www.net-security.org/lm/ads/ads.pl?banner=scannerx1>

Table of contents:

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

[General security news]

CISCO BACKTRACKS ON SECURITY FUNCTIONALITY
Having previously said that it had added firewall and intrusion detection features to its IOS security software, Cisco now said that those features will not actually be integrated into the product until 2003.
>> <http://www.net-security.org/news.php?id=1549>

SECURITY MARKET STILL STRONG
Companies are spending more of their IT budgets on security, according to a study by research firm IDC.
>> <http://www.net-security.org/news.php?id=1550>

LAX SECURITY: ID THEFT MADE EASY
Victims of one of the largest identity theft cases in the United States agree with industry experts that limp security policies at credit bureaus made it easier for the criminals to do their dirty work.
>> <http://www.net-security.org/news.php?id=1551>

AIR FORCE PILOTING SECURE PORTAL
The Air Force is in the initial phases of developing a secure portal

that will provide air operations centers with access to the data they need to make critical warfighting decisions.
>> <http://www.net-security.org/news.php?id=1552>

NATION'S INFRASTRUCTURE FAR FROM SECURE

Ken Watson, the current Cisco Systems executive, is president and chairman of the Partnership for Critical Infrastructure Security. He answers questions related to security.
>> <http://www.net-security.org/news.php?id=1553>

BRUCE SCHNEIER: NO "MAGIC SECURITY DUST"

This is an interview with Bruce Schneier, computer security experts and co-founder of Counterpane Internet Security.
>> <http://www.net-security.org/news.php?id=1554>

SECURITY FIRM DESERTS USERS

Lucira Technologies Inc. has been defunct since August when it filed for bankruptcy. Users say they've never been notified that their managed service has been terminated.
>> <http://www.net-security.org/news.php?id=1555>

CYBERWHOCARES? IT SHOULD!

Is cyberterrorism real? Should corporate IT be worried about it?
>> <http://www.net-security.org/news.php?id=1556>

DOWNLOADABLE EXPLOITS ACCELERATE SECURITY CONCERNS

For hackers or 'script kiddies' to attack and severely damage a Web site or corporate server it's almost a point-and-click exercise using widely available 'downloadable exploits'.
>> <http://www.net-security.org/news.php?id=1559>

ALL EYES ON ELCOMSOFT TRIAL

Opening arguments begin Tuesday in the copyright infringement case against ElcomSoft, a trial expected to test the limits of federal copyright law.
>> <http://www.net-security.org/news.php?id=1560>

WIRELESS NETWORK LAUNCHES AMID SECURITY CONCERNS

Wireless Internet access across Switzerland has moved a step closer to reality with the provision of 100 new locations where the infrastructure is available.
>> <http://www.net-security.org/news.php?id=1561>

DESPITE PRECAUTIONS, NET FRAUD UP

Greater awareness among consumers and merchants has helped deter some online fraud. Trouble is, fraudsters are always updating their methods.
>> <http://www.net-security.org/news.php?id=1562>

HACKER LOG: PATHWAY TO SUCCESSFUL SITE ATTACK

A few fairly simple practices would have prevented my successful

attack on eWeek's OpenHack site. Application security can be attained, but it must be consistently applied and methodically checked to be effective.

>> <http://www.net-security.org/news.php?id=1563>

MAKING WIRELESS LAN SECURITY AIR TIGHT

All-in-one security gateways are helping to boost confidence in wireless networks.

>> <http://www.net-security.org/news.php?id=1564>

LINUX SHOWS POTENTIAL AS IT MEETS SMART CARDS

With the development of smart cards technology mirroring that of the PC development, Linux is also beginning to appear as a contender on the smart card frontier as well.

>> <http://www.net-security.org/news.php?id=1571>

WE HAVE MET THE ENEMY AND HE IS US...

Chet Heath, VP and CTO of Omnicluster, says a company's own worst enemy when it comes to security is itself. In this paper, he describes the implementation of server specific security.

>> <http://www.net-security.org/news.php?id=1572>

U.S. GOVERNMENT FAILS TO MAKE SECURITY GRADE

For the second year running, the federal government has flunked Computer Security 101.

>> <http://www.net-security.org/news.php?id=1573>

AN INTRODUCTION TO DISTRIBUTED DENIAL OF SERVICE ATTACKS

This article will explain the concept of DDoS attacks, how they work, how to react if you become a target, and how the security community can work together to prevent them.

>> <http://www.net-security.org/news.php?id=1574>

VENDORS COMPLETE TOUGHER ICASA 4.0 FIREWALL TESTS

ICSA Labs, which provides one of the most important certifications firewall vendors strive for, said it has completed the first wave of tests of product against version 4.0 of its certification criteria.

>> <http://www.net-security.org/news.php?id=1575>

ASIAN BUSINESSES SPENDING MORE ON INTERNET SECURITY

Businesses in Asia are spending more on Internet security to shield themselves against viruses, external hacking and data corruption, an industry monitor said.

>> <http://www.net-security.org/news.php?id=1576>

SYBASE PATCHES THREE SECURITY HOLES

Sybase has issued a security patch for three vulnerabilities affecting the newest versions of its database software.

>> <http://www.net-security.org/news.php?id=1580>

IDENTITY THEFT MORE OFTEN AN INSIDE JOB

You can take all the steps you want to protect yourself against identity theft: Guard your wallet, shred your personal financial papers before throwing them in the trash, monitor your credit reports.

>> <http://www.net-security.org/news.php?id=1581>

DOES CYBERCRIME STILL PAY?

Jeff Moss, a.k.a. The Dark Tangent and founder of DefCon, the largest annual hacker convention in the United States, said companies no longer hire hackers who have a police record.

>> <http://www.net-security.org/news.php?id=1582>

WHO GOES THERE?

Identity management tools can help CIOs gain control of who gets access to what and when.

>> <http://www.net-security.org/news.php?id=1583>

UK STILL VULNERABLE TO HACKERS

Security experts have rejected claims of a dramatic reduction in hack attacks on the UK last month, maintaining that UK websites are no more secure than others.

>> <http://www.net-security.org/news.php?id=1584>

HOMELAND SECURITY WAITING FOR WI-FI

Security needs to become a priority for users and makers of wireless networking equipment in order to stop insecure connections from being used to attack federal and corporate systems.

>> <http://www.net-security.org/news.php?id=1585>

ETHICS IN DATA MINING AND CRYPTOGRAPHY

In recent years, computer science has become more of an applied science than a pure discipline. It is true that much of the driving force behind proliferation of computing devices is commercial.

>> <http://www.net-security.org/news.php?id=1586>

NEW YEAR TO BRING NASTIER VIRUSES YET

Many odd factors encourage online pests, but businesses should keep up their guard, security expert says.

>> <http://www.net-security.org/news.php?id=1587>

ADOBE: ELCOMSOFT OUTSIDE U.S. LAW

A former piracy investigator for Adobe Systems testifies that he did not tell ElcomSoft to stop selling its eBook-cracking program because he didn't think U.S. copyright law crossed international borders.

>> <http://www.net-security.org/news.php?id=1589>

TROUBLE WITH TROJANS

A security crisis is starting to emerge in the world of computing. The year 2002 will prove to be the worst year yet for malicious

hacking. The following year will probably be worse.
>> <http://www.net-security.org/news.php?id=1590>

CHARGES FILED IN ALLEGED EBAY SCAM

A Los Angeles man was charged on Wednesday with defrauding eBay buyers on six continents in what prosecutors called one of the largest Internet auctions scams uncovered.
>> <http://www.net-security.org/news.php?id=1591>

DOES RESEARCH SUPPORT DUMPING LINUX?

Microsoft's security policies are getting better every day, even as a new report slams open-source competitors as security nightmares. But the easy answers aren't always the right ones.
>> <http://www.net-security.org/news.php?id=1592>

TOWER RECORDS SITE EXPOSES DATA

A security hole on Tower Records' Web site exposed data on millions of U.S. and U.K. customers until it was closed late Wednesday.
>> <http://www.net-security.org/news.php?id=1593>

/ETC/INITTAB - THE MOST OVERLOOKED CRACKER HAVEN

Crackers can cause their software to be run by adding entries to /etc/inittab, a file frequently missed by administrators.
>> <http://www.net-security.org/news.php?id=1595>

2600 AUSTRALIA GOING TO SLEEP

The group's front-man says: "I changed the front page of www.2600.org.au to indicate that 2600 Australia is now in maintenance mode. In other words, we're putting it to sleep."
>> <http://www.net-security.org/news.php?id=1596>

[Vulnerabilities]

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

Apache/Tomcat Denial Of Service And Information Leakage Vulnerability
>> <http://www.net-security.org/vuln.php?id=2281>

akfingerd Multiple Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=2280>

TrendMicro InterScan-VirusWall V3.6 Proxy Vulnerability
>> <http://www.net-security.org/vuln.php?id=2279>

Followup: Shutting Down Sygate Personal Firewall Without
Supplying Password
>> <http://www.net-security.org/vuln.php?id=2278>

Shutting Down Sygate Personal Firewall Without Supplying Password
>> <http://www.net-security.org/vuln.php?id=2277>

SAP Database Symlink Local Root Compromise Vulnerability
>> <http://www.net-security.org/vuln.php?id=2276>

Windows XP Registered AP Information Disclosure Vulnerability
>> <http://www.net-security.org/vuln.php?id=2275>

Vulnerability Report For Linksys Devices
>> <http://www.net-security.org/vuln.php?id=2274>

Vxworks ftpd/3com nbx Denial of Service Vulnerability
>> <http://www.net-security.org/vuln.php?id=2273>

Bypassing Pedestal Software Integrity Protection Driver
>> <http://www.net-security.org/vuln.php?id=2272>

SquirrelMail v1.2.9 Cross Site Scripting Vulnerability
>> <http://www.net-security.org/vuln.php?id=2271>

Local Netfilter / IPTables IP Queue PID Wrap Flaw
>> <http://www.net-security.org/vuln.php?id=2270>

Buffalo Wireless LAN Access Point Denial of Service Vulnerability
>> <http://www.net-security.org/vuln.php?id=2269>

Com21 Cable Modem Configuration File Feeding Vulnerability
>> <http://www.net-security.org/vuln.php?id=2268>

Lawson Financials RDBMS Security Issue
>> <http://www.net-security.org/vuln.php?id=2267>

ShopFactory Shopping Cart Price Manipulation Vulnerability
>> <http://www.net-security.org/vuln.php?id=2266>

YaBB 1 Gold - SP1 Cross Site Scripting Vulnerability
>> <http://www.net-security.org/vuln.php?id=2265>

Multiple pServ Remote Buffer Overflow Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=2264>

Moby NetSuite POST Denial of Service Vulnerability
>> <http://www.net-security.org/vuln.php?id=2263>

Bogofilter Contrib/Bogopass Temp File Vulnerability
>> <http://www.net-security.org/vuln.php?id=2262>

[Advisories]

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

SuSE Security Announcement - OpenLDAP2
>> <http://www.net-security.org/advisory.php?id=1369>

SCO Security Advisory - Linux: apache vulnerabilities in shared memory, DNS, and ApacheBench
>> <http://www.net-security.org/advisory.php?id=1368>

SGI Security Advisory - BIND Name Server DNS Spoofing Vulnerability
>> <http://www.net-security.org/advisory.php?id=1367>

SGI Security Advisory - BIND Name Server DNS Spoofing Vulnerability
>> <http://www.net-security.org/advisory.php?id=1366>

Debian Security Advisory - New kdlibs packages fix arbitrary program execution
>> <http://www.net-security.org/advisory.php?id=1365>

Red Hat Security Advisory - Updated Webalizer packages fix vulnerability
>> <http://www.net-security.org/advisory.php?id=1364>

Microsoft Security Bulletin MS02-068 - Cumulative Patch for Internet Explorer
>> <http://www.net-security.org/advisory.php?id=1363>

Microsoft Security Bulletin MS02-067 - E-mail Header Processing Flaw Could Cause Outlook 2002 to Fail
>> <http://www.net-security.org/advisory.php?id=1362>

SGI Security Advisory - Buffer Overflow Vulnerability in X
Font Server

>> <http://www.net-security.org/advisory.php?id=1361>

SGI Security Advisory - Multiple Vulnerabilities in BIND
Name Service Daemon

>> <http://www.net-security.org/advisory.php?id=1360>

SCO Security Advisory - Linux: RPC XDR buffer overflow

>> <http://www.net-security.org/advisory.php?id=1359>

SCO Security Advisory - Linux: exploitable memory leak in ypserv

>> <http://www.net-security.org/advisory.php?id=1358>

Conectiva Linux Security Announcement - pine

>> <http://www.net-security.org/advisory.php?id=1357>

Debian Security Advisory - New smb2www packages fix
arbitrary command execution

>> <http://www.net-security.org/advisory.php?id=1356>

Red Hat Security Advisory - Updated KDE packages fix security issues

>> <http://www.net-security.org/advisory.php?id=1355>

Red Hat Security Advisory - Updated Webalizer packages
fix vulnerability

>> <http://www.net-security.org/advisory.php?id=1354>

Red Hat Security Advisory - Updated xinetd packages fix
denial of service vulnerability

>> <http://www.net-security.org/advisory.php?id=1353>

Mandrake Linux Security Advisory - WindowMaker

>> <http://www.net-security.org/advisory.php?id=1352>

Mandrake Linux Security Advisory - pine

>> <http://www.net-security.org/advisory.php?id=1351>

Debian Security Advisory - New IM packages fix insecure
temporary file creation

>> <http://www.net-security.org/advisory.php?id=1350>

Red Hat Security Advisory - Updated xinetd packages
fix denial of service

>> <http://www.net-security.org/advisory.php?id=1349>

OpenPKG Security Advisory - samba
>> <http://www.net-security.org/advisory.php?id=1348>

Debian Security Advisory - New Free/SWan packages
fix denial of service
>> <http://www.net-security.org/advisory.php?id=1347>

Gentoo Linux Security Announcement - pine
>> <http://www.net-security.org/advisory.php?id=1346>

[Featured articles]

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

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

PC GUARDIAN RELEASES ENCRYPTION PLUS EMAIL 3.0
Encryption Plus Email 3.0, enterprise software uses public-private key technology to automatically encrypt and decrypt email messages between users.
>> <http://www.net-security.org/article.php?id=285>

S/MIME - THE REALITY OF INTEROPERABILITY
People assume that when they buy an S/MIME compliant email application they can send digitally signed and encrypted emails to any other S/MIME compatible client. The reality however is somewhat different...
>> <http://www.net-security.org/article.php?id=286>

REEFEDGE LICENSES SSH SENTINEL VPN CLIENT
ReefEdge, Inc. has licensed the SSH Sentinel 1.4 VPN client software for secure access with the ReefEdge Connect System 3.0, the latest security and management solution for Wireless Local Area Networks.
>> <http://www.net-security.org/article.php?id=287>

REPORT ON MICROSOFT WINDOWS ENCRYPTING FILE SYSTEM
Network Associates has published an analysis of the architecture, use and security of the Microsoft Windows Encrypting File System.
>> <http://www.net-security.org/article.php?id=288>

PGP CORP. RELEASES PGP 8.0 FOR WINDOWS AND MACINTOSH
PGP Corporation today announced the release of several eagerly awaited products - PGP Enterprise 8.0, PGP Desktop 8.0 and PGP Personal 8.0 for Windows and Macintosh.

>> <http://www.net-security.org/article.php?id=289>

SOURCE CODE FOR PGP 8.0 RELEASED

Simultaneously with today's release of PGP 8.0 for Windows and Macintosh, PGP Corporation announced the availability of PGP 8.0 source code.

>> <http://www.net-security.org/article.php?id=290>

QUALYS CTO RECEIVES INDUSTRY RECOGNITION

The next issue of InfoWorld Magazine will present in-depth profiles of this year's "25 Most Influential CTOs". One of the "chosen ones" is Gerhard Eschelbeck, CTO and VP of Engineering, Qualys, Inc.

>> <http://www.net-security.org/article.php?id=291>

PERMEO APPLICATION SECURITY PLATFORM SHOWCASE

Permeo Technologies, one of the key players in the application security field will exhibit the latest version of its Permeo Application Security Platform at the 2002 InfoSecurity conference and show in NYC.

>> <http://www.net-security.org/article.php?id=292>

5-FACTOR ANTIVIRUS SYSTEM FOR EXCHANGE LAUNCHED

800onemail Inc., a company that provides 24x7x365 managed e-mail and Exchange services, launched a 5-Factor Antivirus system for Exchange business email.

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

VERISIGN ANNOUNCES TRUSTED CONTENT DELIVERY FOR SOFTWARE PROVIDERS

VeriSign, Inc. announced it will be providing a Trusted Content Delivery service for software providers that creates a secure distribution channel for sending software programs and updates over the Internet.

>> <http://www.net-security.org/article.php?id=294>

NEW WEB SEMINAR FROM SOPHOS

On Tuesday December 10th, 2002 Sophos will host a web seminar titled "Safe computing: Anti-virus Software Alone is not Enough".

>> <http://www.net-security.org/article.php?id=295>

[**Security world**]

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

SafeGuard Advanced Security: Modules for a Targeted and Cost
Effective Increase of the IT Security Level

>> <http://www.net-security.org/press.php?id=1154>

Analyst Firm Ranks NetScreen the Fastest Growing Security
Appliance Vendor in VPN & Firewall Market

>> <http://www.net-security.org/press.php?id=1153>

PromiseMark Includes BitDefender in its Virus Protection Plan

>> <http://www.net-security.org/press.php?id=1152>

GFI's New LANguard S.E.L.M. 4 Combats Intruders

>> <http://www.net-security.org/press.php?id=1151>

Tel.Net Media Issues Wake up Call to Company Directors
Over IT Security

>> <http://www.net-security.org/press.php?id=1150>

Klez Worm is Most Prolific Virus of the Year

>> <http://www.net-security.org/press.php?id=1149>

Colorado DOR Enhances License Issuance Program with Automated
Facial Recognition Technology to Reduce Identity Fraud

>> <http://www.net-security.org/press.php?id=1148>

SUNDAY Partners With Hongkong Post and Diversinet to
Promote Secure M-Commerce

>> <http://www.net-security.org/press.php?id=1147>

Snapgear Launches Powerful New Small-Medium Enterprise
Range Of VPN Firewall Appliances

>> <http://www.net-security.org/press.php?id=1146>

Mobiletech Selects Diversinet's Wireless Security For Its
Mobile Productivity Products

>> <http://www.net-security.org/press.php?id=1145>

nCipher Chosen to Provide Transaction Security and
Database Encryption for Exostar

>> <http://www.net-security.org/press.php?id=1144>

Panda Antivirus Beta now Available for Windows .NET Servers
>> <http://www.net-security.org/press.php?id=1143>

Zone Labs Integrity 2.0 Endpoint Security Now Available
>> <http://www.net-security.org/press.php?id=1142>

GFI Offers WebMonitor for ISA Server as Freeware
>> <http://www.net-security.org/press.php?id=1141>

[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

CLEAN DISK SECURITY 6.2 (Windows)
This program gives you secure file deletion, making sure that deleted files cannot be undeleted again. Deleting a file normally just removes the file's directory entry, but the data itself remains on the disk.
>> <http://www.net-security.org/software.php?id=385>

PC SECURITY 5.1 (Windows)
This program offers multiple locking systems for the Windows environment and the Internet. Lock files, monitor programs activities, even detect intruders! PC Security offers flexible and complete password protection, "Drag and Drop" support, plus many other handy features.
>> <http://www.net-security.org/software.php?id=386>

STEALTH ENCRYPTOR 5.0 (Windows)
Stealth Encryptor is a powerful PC encryption program. Users can quickly render sensitive files and e-mail totally unreadable with a user specified password.
>> <http://www.net-security.org/software.php?id=387>

VEXIRA ANTIVIRUS 2.0 (Linux)
A complete virus defense system designed for easy and dependable virus prevention on Linux based servers. Vexira Antivirus uses an advanced multi-platform virus inspection technology.
>> <http://www.net-security.org/software.php?id=388>

SOLO ANTIVIRUS 2.5 (Windows)

Solo Antivirus detects and disinfects all types of viruses. It contains a unique system integrity checker to protect your system from New Internet worms, Backdoors and Spy tools.

>> <http://www.net-security.org/software.php?id=389>

COM-GUARD LOCAL 2.2 (Windows)

Com-Guard Local 2.2 acts as a virtual computer safe where your important files are securely kept. It raises your computer's security to a level that is well above that offered by your Windows operating system.

>> <http://www.net-security.org/software.php?id=390>

YAFIG 0.2 (Linux)

Yafig is a LAMP-based firewall rule generator that creates shell scripts for use with Linux netfilter/iptables. The user interface is similar to the FireWall-1 policy editor.

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

OUBLIETTE 1.5 (Windows)

This program will store a list of accounts with information such as account name, associated password, URL, and free-form notes. You can easily access the information, copy to clipboard or export to a variety of formats (text, HTML, comma-separated or Windows INI).

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

SPAMWEASEL 1.0.18 (Windows)

This junkmail-busting freeware utility will K.O. spam according to both objective and personal criteria, deleting or archiving it while placing an optional warning notice on any suspected spam mail it allows through to your mailbox.

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

PERL SECUREPAGES 0.0.1 (Linux)

Perl SecurePages is an attempt at a method to secure perl CGI on a session basis. The Current release of Perl SecurePages (PSBAS) offers protection of perl CGI applications based on user and group requirements, a web based admin tool, and a MySQL back-end.

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

[Virus News]

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

Weekly Virus Report - Pheme and Lagel Worms, DobeA Trojan
and Julso Macro Virus
>> http://www.net-security.org/virus_news.php?id=139

Panda Reports the Appearance of the Lagel.A Worm
>> http://www.net-security.org/virus_news.php?id=138

Panda Antivirus Beta for Windows .NET Servers
>> http://www.net-security.org/virus_news.php?id=137

Kaspersky Labs: Virus Top 20 for November 2002
>> http://www.net-security.org/virus_news.php?id=136

Central Command: Top 12 Viruses For November 2002
>> http://www.net-security.org/virus_news.php?id=135

Top Ten Viruses Detected by Panda ActiveScan in November
>> http://www.net-security.org/virus_news.php?id=134

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

SECURITY INCIDENT ALERT

Check your Web servers, FTP servers, Mail servers , DNS servers,
firewalls, IDS systems, switchers and routers for over 900 up to
date vulnerabilities. Secure your critical assets today!

FREE System Security Test and Detailed Report
<http://www.net-security.org/lm/ads/ads.pl?banner=scannerx1>
