



Newsletter
Issue 136

Issue 136 - 18.10.2002

<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>.

Bulletproof Your Network: FREE Guide

Existing security products -- firewalls, anti-virus and IDS -- are simply no longer enough to ensure your networks are safe against sophisticated attacks and worms such as Code Red and Nimda.

FREE Guide shows you how to ensure TOTAL security for your network. Get it now.

https://www.qualys.com/forms/nsguideh_426.php

Table of contents:

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

[General security news]

5 STEPS TO SECURE MOBILE DATA

Mobile and wireless technology is revolutionising how businesses use and profit from information.

>> <http://www.net-security.org/news.php?id=1414>

SMALL FIRMS WARNED OVER ATTACKERS

Smaller businesses do not have adequate defences against the increasing threat from electronic attacks by terrorists, the British Chambers of Commerce has warned.

>> <http://www.net-security.org/news.php?id=1415>

STONES, FIRE AND WATER

A nasty trade secret lawsuit displays the ugly side of the network security industry...

>> <http://www.net-security.org/news.php?id=1416>

SECURE TWICE, OPEN ONCE

The increasing popularity of VPN technology has exposed a number of serious vulnerabilities in the software used to connect thousands of remote offices and workers to their corporate networks.

>> <http://www.net-security.org/news.php?id=1417>

FEDS CONSIDER NEW SECURITY REPORTING ROLE

Government security officials have been discussing the possibility of creating a central point of contact within the government for reporting security vulnerabilities.

>> <http://www.net-security.org/news.php?id=1418>

ARE MACS VIRUS-PROOF?

Mac OS X users should install an effective, configurable firewall, which comes included with a point-and-click interface in OS 10.2, also known as Jaguar.

>> <http://www.net-security.org/news.php?id=1419>

US CRACKS CASE OF ATTACKER WHO BROKE INTO MILITARY NETWORKS

Federal authorities have cracked the case of an international attacker who broke into roughly 100 unclassified U.S. military networks over the past year.

>> <http://www.net-security.org/news.php?id=1424>

ANTENNA TO BOOST WIRELESS SECURITY

An optical antenna that uses a geometrically shaped lens promises to bring greater security to wireless networks for businesses, according to British scientists.

>> <http://www.net-security.org/news.php?id=1425>

TECHNOLOGY HACKERS BEWARE: QUANTUM ENCRYPTION IS COMING

Quantum encryption pioneers promise to put the world's first uncrackably secure networks online by early 2003.

>> <http://www.net-security.org/news.php?id=1426>

COMPUTER BREAK-INS: YOUR RIGHT TO KNOW

California law now demands that the public be informed when government or corporate databases are breached. It's about time.

>> <http://www.net-security.org/news.php?id=1427>

PLAN FOR A SECURITY ARCHITECTURE

An architecture-based approach to information security will reduce legal liability and improve the efficiency of security initiatives.

>> <http://www.net-security.org/news.php?id=1428>

NEW SPAM CONTROL ADDED TO MXTREME MAIL FIREWALL

BorderWare Technologies Inc. announced today a new weapon in the war against spam and unwanted email. This is the latest innovation to the MXtreme Mail Firewall range of appliances.

>> <http://www.net-security.org/news.php?id=1429>

SECURITY WARNING ON OPEN SOURCE

Linux is not a more secure environment than NT or Windows, Internet Security Systems chief technology officer Chris Klaus warns.

>> <http://www.net-security.org/news.php?id=1430>

WEB DESIGNER CHARGED WITH VIRUS WRITING AND CHILD PORN OFFENCES

A 21-old Welsh Web designer has appeared in court charged with creating and distributing three mass mailer viruses.

>> <http://www.net-security.org/news.php?id=1434>

MAKE NESSUS YOUR NEW SECURITY TOOL OF CHOICE

No ace sysadmin should be without Nessus, it's the utility of choice for hardcore security scanning.

>> <http://www.net-security.org/news.php?id=1435>

TROJAN FOUND IN LIBPCAP AND TCPDUMP

Members of The Houston Linux Users Group discovered that the newest sources of libpcap and tcpdump available from tcpdump.org were contaminated with trojan code.

>> <http://www.net-security.org/news.php?id=1436>

WEB IDENTITY: WEIGHING THE ALTERNATIVES

Microsoft's Passport and Liberty Alliance specify incompatible authentication technologies today. Here's how they work - and how they might interoperate in the future.

>> <http://www.net-security.org/news.php?id=1438>

CONGRESS OKS CYBER SECURITY GRANTS

Congress approved Tuesday \$903 million in grants to spur federal agencies, industry and universities to devote more energy to cyber security research.

>> <http://www.net-security.org/news.php?id=1439>

ENCRYPTED NFS WITH OPENSSSH AND LINUX

NFS is a protocol that allows computers to share files over a network. It has several security related problems. This article provides a solution to most of these problems for Linux clients and servers.

>> <http://www.net-security.org/news.php?id=1440>

MICROSOFT HIRES NATIONAL SECURITY ADVISOR

Hoping to play a larger role in homeland security, Microsoft has tapped former US political adviser Thomas Richey for a new position counselling policymakers on IT issues.

>> <http://www.net-security.org/news.php?id=1444>

HOUSE VOTES LIFE SENTENCES FOR HACKERS

A last-minute addition to a proposal for a Department of Homeland Security would punish malicious hackers with life in prison.

>> <http://www.net-security.org/news.php?id=1445>

BACK TO THE INSECURE FUTURE

Web services, such as Microsoft's .NET platform, represent a return to centralized computing. But that's not all, they also pose some serious security issues.

>> <http://www.net-security.org/news.php?id=1446>

MAINTAINING CREDIBLE IIS LOG FILES

This article will offer advice on how to maintain the credibility of IIS log files.

>> <http://www.net-security.org/news.php?id=1447>

WEP IS OUT, WPA IS IN

Wi-Fi Protected Access (WPA) will replace Wired Equivalent Privacy (WEP), which presents security concerns on wireless LANs. Enterprises should install WPA as soon as it becomes available.

>> <http://www.net-security.org/news.php?id=1448>

UK MALICIOUS HACKER TO FIGHT US EXTRADITION

A British man wanted in the US for allegedly hacking into nearly 100 computer networks operated by the US military and Nasa has said he will fight any attempt to extradite him.

>> <http://www.net-security.org/news.php?id=1449>

THE UNIX AUDITOR'S PRACTICAL HANDBOOK

This is a step-by-step practical guide to auditors when carrying out a Unix Audit. It mostly covers Sun Solaris systems, but it has cross-references for AIX and Linux.

>> <http://www.net-security.org/news.php?id=1450>

THE WORST SECURITY PROBLEMS?

The FBI list is misleading in that many readers and editors would have seen this as an FBI certification of the relative equality of security problems between systems running Windows and those running Unix.

>> <http://www.net-security.org/news.php?id=1453>

REVERSE ENGINEERING WIN32 TROJANS ON LINUX

This article offers a detailed examination of the reversing process, using a trojan found in the wild, and focusing on techniques for reversing Windows-native code entirely under Linux.

>> <http://www.net-security.org/news.php?id=1454>

RUSSIANS WAGE CYBER WAR ON CHECHEN WEB SITES

Two Chechen news Web sites collapsed after an alleged coordinated cyber attack from Russian security services.

>> <http://www.net-security.org/news.php?id=1455>

[Vulnerabilities]

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

Well Known Flaw in Web Cart Software Remains Wide Open
>> <http://www.net-security.org/vuln.php?id=2224>

Yahoo, Hotmail and Excite Web Mail Cross Site
Scripting Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=2223>

KeyFocus KF Web Server File Disclosure Vulnerability
>> <http://www.net-security.org/vuln.php?id=2222>

Macromedia ColdFusion/JRun Remote SYSTEM Buffer
Overflow Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=2221>

APBoard Multiple Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=2220>

INweb Mail Server v2.01 Denial of Service Vulnerability
>> <http://www.net-security.org/vuln.php?id=2219>

Hyperion Ftp Server v2.8.1 Directory Traversal Vulnerability
>> <http://www.net-security.org/vuln.php?id=2218>

XOOPS RC3 WebChat Module SQL Injection Vulnerability
>> <http://www.net-security.org/vuln.php?id=2217>

RhinoSoft Serv-U FTP Anonymous Remote DoS Vulnerability
>> <http://www.net-security.org/vuln.php?id=2216>

Multiple Remote Vulnerabilities in BIND4 and BIND8
>> <http://www.net-security.org/vuln.php?id=2215>

KDE resLISa Buffer Overflow Vulnerability
>> <http://www.net-security.org/vuln.php?id=2214>

Tiny HTTPd Multiple Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=2213>

iSMTP Gateway Buffer Overflow Vulnerability
>> <http://www.net-security.org/vuln.php?id=2212>

xoops Quizz Module IMG Vulnerability
>> <http://www.net-security.org/vuln.php?id=2211>

eZ httpbench v.1.1 Arbitrary File Disclosure Vulnerability
>> <http://www.net-security.org/vuln.php?id=2210>

QNX Neutrino RTOS Non-Explicit Path Vulnerability
>> <http://www.net-security.org/vuln.php?id=2209>

Simple Web Server File Disclosure Vulnerability
>> <http://www.net-security.org/vuln.php?id=2208>

Zeus Admin Server v4.1r2 index.fcgi Cross Site Scripting Vulnerability
>> <http://www.net-security.org/vuln.php?id=2207>

Postnuke Rogue Release (0.72) Cross Site Scripting Vulnerability
>> <http://www.net-security.org/vuln.php?id=2206>

LiteServe Directory Index Cross Site Scripting Vulnerability
>> <http://www.net-security.org/vuln.php?id=2205>

[Advisories]

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

Compaq Security Bulletin - OSIS V5.4 LDAP Module for System Authentication Potential Security Vulnerability
>> <http://www.net-security.org/advisory.php?id=1288>

Compaq Security Bulletin - HP Tru64 UNIX IGMP Potential (DoS) Security Vulnerability
>> <http://www.net-security.org/advisory.php?id=1287>

Compaq Security Bulletin - HP TruCluster Server Interconnect Potential Security Vulnerability
>> <http://www.net-security.org/advisory.php?id=1286>

FreeBSD Security Advisory - buffer overrun in resolver
>> <http://www.net-security.org/advisory.php?id=1285>

SCO Security Advisory - Linux: buffer overflows and other security issues in squid
>> <http://www.net-security.org/advisory.php?id=1284>

SCO Security Advisory - Linux: python insecure temporary files in os._execvpe
>> <http://www.net-security.org/advisory.php?id=1283>

Mandrake Linux Security Advisory - bind
>> <http://www.net-security.org/advisory.php?id=1282>

Debian Security Advisory - New BIND packages fix several vulnerabilities
>> <http://www.net-security.org/advisory.php?id=1281>

Conectiva Linux Security Announcement - bind
>> <http://www.net-security.org/advisory.php?id=1280>

Red Hat Security Alert - Remote vulnerabilities in BIND 4 and 8
>> <http://www.net-security.org/advisory.php?id=1279>

SuSE Security Announcement - bind8
>> <http://www.net-security.org/advisory.php?id=1278>

CERT Advisory CA-2002-31 - Multiple Vulnerabilities in BIND
>> <http://www.net-security.org/advisory.php?id=1277>

Conectiva Linux Security Announcement - php4
>> <http://www.net-security.org/advisory.php?id=1276>

CERT Advisory CA-2002-30 - Trojan Horse tcpdump and libpcap Distributions
>> <http://www.net-security.org/advisory.php?id=1275>

Debian Security Advisory - New Apache-Perl packages fix several vulnerabilities
>> <http://www.net-security.org/advisory.php?id=1274>

EnGarde Secure Linux Advisory - bind-chroot, bind-chroot-utils
>> <http://www.net-security.org/advisory.php?id=1273>

Gentoo Linux Security Announcement - kdenetwork
>> <http://www.net-security.org/advisory.php?id=1272>

Gentoo Linux Security Announcement - kdelibs
>> <http://www.net-security.org/advisory.php?id=1271>

FreeBSD Security Advisory - multiple vulnerabilities in BIND
>> <http://www.net-security.org/advisory.php?id=1270>

FreeBSD Security Advisory - Buffer overflow in kadmind daemon
>> <http://www.net-security.org/advisory.php?id=1269>

SGI Security Advisory - Apache Security Vulnerabilities
>> <http://www.net-security.org/advisory.php?id=1268>

SCO Security Advisory - UnixWare 7.1.1 Open UNIX 8.0.0:
in.talkd format string vulnerabilities
>> <http://www.net-security.org/advisory.php?id=1267>

SGI Security Advisory - IRIX lpd daemon vulnerabilities
via sendmail and dns
>> <http://www.net-security.org/advisory.php?id=1266>

NetBSD Security Advisory - IPFilter FTP proxy
>> <http://www.net-security.org/advisory.php?id=1265>

SCO Security Advisory - Linux: libpng progressive image
loading vulnerabilities and other buffer overflows
>> <http://www.net-security.org/advisory.php?id=1264>

Debian Security Advisory - New masqmail packages
fix buffer overflows
>> <http://www.net-security.org/advisory.php?id=1263>

Novell Security Advisory - Remote Manager Security Issue - eDir 8.6.2
>> <http://www.net-security.org/advisory.php?id=1262>

Novell Security Advisory - Remote Manager Security Issue - NW5.1
>> <http://www.net-security.org/advisory.php?id=1261>

Gentoo Linux Security Announcement - apache
>> <http://www.net-security.org/advisory.php?id=1260>

KDE Security Advisory - resLISa / LISa Vulnerabilities
>> <http://www.net-security.org/advisory.php?id=1259>

KDE Security Advisory - rlogin.protocol and telnet.protocol
URL KIO Vulnerability
>> <http://www.net-security.org/advisory.php?id=1258>

SuSE Security Announcement - traceroute-nanog/nkitb
>> <http://www.net-security.org/advisory.php?id=1257>

SuSE Security Announcement - kdenetwork
>> <http://www.net-security.org/advisory.php?id=1256>

Red Hat Security Advisory - New PHP packages fix
vulnerability in mail function
>> <http://www.net-security.org/advisory.php?id=1255>

Debian Security Advisory - New klisa packages fix buffer overflow
>> <http://www.net-security.org/advisory.php?id=1254>

SCO Security Advisory - Linux: Preboot eXecution Environment
(PXE) server denial-of-service attacks
>> <http://www.net-security.org/advisory.php?id=1253>

Novell Security Advisory - iManager (eMFrame) Buffer Overflow
>> <http://www.net-security.org/advisory.php?id=1252>

Gentoo Linux Security Announcement - kggg
>> <http://www.net-security.org/advisory.php?id=1251>

Debian Security Advisory - squirrelmail (update)
>> <http://www.net-security.org/advisory.php?id=1250>

Debian Security Advisory - New html2ps packages fix
arbitrary code execution
>> <http://www.net-security.org/advisory.php?id=1249>

Mandrake Linux Security Advisory - perl-MailTools
>> <http://www.net-security.org/advisory.php?id=1248>

Mandrake Linux Security Advisory - nss_ldap
>> <http://www.net-security.org/advisory.php?id=1247>

[Featured articles]

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

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

Spoofing - Arts of attack and defense
>> <http://www.net-security.org/article.php?id=262>

Explaining encryption
>> <http://www.net-security.org/article.php?id=261>

How do you deal with Internet fraud?
>> <http://www.net-security.org/article.php?id=260>

Bind Security Vulnerabilities Roundup
>> <http://www.net-security.org/article.php?id=259>

The changing face of web security
>> <http://www.net-security.org/article.php?id=258>

What makes a good Password?
>> <http://www.net-security.org/article.php?id=257>

An introduction to PKI
>> <http://www.net-security.org/article.php?id=256>

Layer 2 Analysis of WLAN Discovery Applications for
Intrusion Detection
>> <http://www.net-security.org/article.php?id=255>

Timing the Application of Security Patches for Optimal Uptime
>> <http://www.net-security.org/article.php?id=254>

Host Discovery with nmap
>> <http://www.net-security.org/article.php?id=253>

Vulnerabilities in Microsoft's Java implementation
>> <http://www.net-security.org/article.php?id=252>

New NetScreen-5XT features increase security for remote sites
>> <http://www.net-security.org/article.php?id=251>

[**Security world**]

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

Baltimore secures DigiNotar's 'DigiOverheid' Service for Issuing
Digital Certificates to End Users in the Netherlands
>> <http://www.net-security.org/press.php?id=1118>

Network Associates Extends Leadership Position with McAfee
Online Managed Security Services
>> <http://www.net-security.org/press.php?id=1117>

Network Associates Expert Services Organization Expands
Security Educational Offerings
>> <http://www.net-security.org/press.php?id=1116>

PureEdge Announces Support for XForms
>> <http://www.net-security.org/press.php?id=1115>

TriGeo Unveils Future of Security Information Management
at 29th Annual CSI Show
>> <http://www.net-security.org/press.php?id=1114>

New Report says Rainbow's iKey is the Worldwide Market Share
Leader for USB Authentication Keys
>> <http://www.net-security.org/press.php?id=1113>

RSA Security Combines Building and Network Access With New
RSA Smart Badging Solution
>> <http://www.net-security.org/press.php?id=1112>

NetContinuum Transforms Enterprise Security Market With
Introduction of All-in-One Web Security Gateway
>> <http://www.net-security.org/press.php?id=1111>

Neoteris Unveils Next-Generation Secure Access Product Family
of Instant Virtual Extranets
>> <http://www.net-security.org/press.php?id=1110>

Information Security Editor-in-Chief To Lead Special Keynote
Panel at Comdex Fall 2002
>> <http://www.net-security.org/press.php?id=1109>

New NetScreen-5XT Features Enhance Security and Resiliency for Remote Sites

>> <http://www.net-security.org/press.php?id=1108>

Intrusion Inc. Applies to Transfer to Nasdaq SmallCap Market

>> <http://www.net-security.org/press.php?id=1107>

[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

FILEASSURITY 1.3.0 (Windows)

FileAssurity is an easy to use, low cost, PKI enabled file encryption application that enables you to securely protect and sign your files for storage or sending.

>> <http://www.net-security.org/software.php?id=355>

SOFTCLAN E-CRYPTOR 1.7 (Windows)

- Quickly and Easily send Encrypted Emails that need nothing but the password to decrypt

- Encrypt Sensitive Files and Folders on your hard drive or removable media

- Encrypt Back-up Files

>> <http://www.net-security.org/software.php?id=356>

HOTCRYPT 4.1.2 (Windows)

With HotCrypt running on your computer, you can easily make text within any window unreadable for other people.

>> <http://www.net-security.org/software.php?id=357>

FILTERTOOLS 1.0 (Linux)

FilterTools is an easy to use SQL driven Web- based solution for keeping people out of an unsecured 802.11b wireless network or shared wired networks.

>> <http://www.net-security.org/software.php?id=358>

EMC 8.16 (Windows)

EmC (Email Control) is an anti-spam tool that allows you to reduce the number of junk mails arriving in your inbox. The program works with a combination of filters, that can be customized by the user and checks the mail while it is still

on your ISPs server.

>> <http://www.net-security.org/software.php?id=359>

CLIPSECURE 1.1 (Windows)

ClipSecure is a simple, secure freeware text encryption utility that operates with the Windows clipboard, and therefore can be used with any text-based program and most email clients.

>> <http://www.net-security.org/software.php?id=360>

FREECRYPT32 (Windows)

This tool allows you to encrypt (lock) your files with a password. The file becomes completely useless until it is decrypted with the password.

>> <http://www.net-security.org/software.php?id=361>

TVARK 0.3 (Linux)

Tvark is a network monitoring tool (sniffer) with a GUI front end and is tied to a MySQL database. The GUI provides a view of traffic activity that can be seen from the machine/interface that Tvark is run on.

>> <http://www.net-security.org/software.php?id=362>

FWM 1.5.3 (Linux)

FWM is the answer to a large gap in management of linux firewalls. It manages network configuration, initialization, interfaces, routing, nat, and policy configuration. It is not meant to be a replacement or front end to iptables, as it requires an iptables policy and nat file (templates included).

>> <http://www.net-security.org/software.php?id=363>

WOLVERINE FIREWALL 99B2 (Linux)

Wolverine Firewall is a prompt-driven firewall configurator for IPTABLES. Wolverine Firewall prompts you for ports that you would like to leave open, but will also help you to restrict access to and from specific IP addresses.

>> <http://www.net-security.org/software.php?id=364>

[Virus News]

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

Norman Virus Control Receives Virus Bulletin 100% Award
>> http://www.net-security.org/virus_news.php?id=123

Creator of Gokar and Redesi Worms Faces Charges
>> http://www.net-security.org/virus_news.php?id=122

Fourth Anniversary of Bubbleboy and Self Executing Viruses
>> http://www.net-security.org/virus_news.php?id=121

Your Mobile Phone Is Safe - "Ace-?" is a Hoax
>> http://www.net-security.org/virus_news.php?id=120

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

Bulletproof Your Network: FREE Guide

Existing security products -- firewalls, anti-virus and IDS -- are simply no longer enough to ensure your networks are safe against sophisticated attacks and worms such as Code Red and Nimda.

FREE Guide shows you how to ensure TOTAL security for your network. Get it now.

https://www.qualys.com/forms/nsguideh_426.php
