



HNS Newsletter

Issue 196 - 19.01.2004.

<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.

FREE GUIDE-128-bit encryption

Thawte is one of the few companies that offers 128 bit supercerts. A supercert will allow you to extend the highest allowed 128 bit encryption to all your clients even if they use browsers that are limited to 40 bit encryption.

Download a guide to learn more.

<http://ad.doubleclick.net/clk;6091071;8369141;h>

Table of contents:

- 1) Security news
- 2) Vulnerabilities
- 3) Advisories
- 4) Articles
- 5) Reviews
- 6) Software
- 7) Webcasts
- 8) Conferences
- 9) Security world

[Security news]

LOCKING YOUR DOOR IN 2004

Teach your users to think as you do... and other resolutions for the new year.

<http://www.net-security.org/news.php?id=4381>

WHEN A SECURITY FEATURE IS NO LONGER SECURE

Question: When is a security feature not a security feature?

Answer: When it's the document protection system in Microsoft Word.

<http://www.net-security.org/news.php?id=4382>

NEW TROJAN MASQUERADES AS WINDOWS XP UPDATE

Security companies are warning Internet users about a new Trojan horse program spreading via spam e-mail and masquerading as a Windows XP software update from Microsoft.
<http://www.net-security.org/news.php?id=4383>

SCHOOL DISTRICT GIVES LINUX SECURITY TECHNOLOGY HIGH GRADES

As any corporate IT administrator knows, network security is no longer a luxury, but a necessity.
<http://www.net-security.org/news.php?id=4384>

BUSINESS CONTINUITY PLANNING: WILL IT SAVE YOU?

Every year, security firm Pinkerton publishes a survey of the top threats that businesses believe that they have faced over that particular year writes Fran Howarth of Bloor Research.
<http://www.net-security.org/news.php?id=4385>

'SERIAL ID THIEVES' BANNED FROM AUCTION SITES

A US Federal Court last week imposed an order prohibiting two alleged ID fraudsters from taking part in Internet auctions.
<http://www.net-security.org/news.php?id=4387>

DIGITAL SIGNATURES AND EUROPEAN LAWS

People who do business on the Internet require security and trust. In electronic commerce and communication you can't see the person you are speaking with, you can't see the documents that prove one's identity, and you can't even know if the web site you are connected to belongs to the society it says.
<http://www.net-security.org/news.php?id=4388>

IS THE TIDE TURNING IN BATTLE AGAINST HACKERS?

It's a quagmire. No, not Iraq. The Internet. The war against hackers has been going on for decades and we are no closer to pulling out than we were when Kevin Mitnick was breaking into Ma Bell's mainframes in the early '80s.
<http://www.net-security.org/news.php?id=4389>

MICROSOFT FOCUSES IDENTITY-MANAGEMENT EFFORT

Amid the growing buzz around identity management, Microsoft is trying to pull together a platform that would offer corporations entry into a new generation of end-user management, security and regulatory compliance.
<http://www.net-security.org/news.php?id=4390>

ENGAGING IN WORM WARFARE

Last summer, it seemed the onslaught would never end. One after another, a progression of worms and other malware threatened to bring down systems as enterprises floundered in a morass of unpatched vulnerabilities and malicious e-mails

opened by unwary employees.
<http://www.net-security.org/news.php?id=4391>

RADIO HACKERS HURL DRIVE BY ABUSE AT BURGER KING CUSTOMERS

Burger King customers visiting a drive-through restaurant had to run a gamut of abuse after pranksters succeeded in hacking into the outlet's wireless intercom system.
<http://www.net-security.org/news.php?id=4392>

HACKERS ATTACK THE OU HEALTH SCIENCES CENTER

Federal and state law enforcement agencies are investigating a computer-hacking incident of 25 to 30 Microsoft Windows and Unix computers and servers at the OU Health Sciences Center.
<http://www.net-security.org/news.php?id=4393>

IT IN 2004: MORE POWER, LOWER COSTS AND SECURE

Higher performance, lower costs and stronger security will be the key drivers for the IT industry during 2004.
<http://www.net-security.org/news.php?id=4395>

THE EIGHT RULES OF SECURITY

Security is a process, not a product... and should be treated as such. Through the security lifecycle, policy and procedure needs to take precedence over implementation. It's a bigger part of the circle for a reason.
<http://www.net-security.org/news.php?id=4396>

ALERT ADMIN GETS BANK SCAM SITE SHUT DOWN

An alert systems integration manager in Melbourne got a fake banking site targeting Westpac last week shut down. The site was being hosted on an internet-connected computer without the knowledge of the owner.
<http://www.net-security.org/news.php?id=4397>

IDENTITY THEFT IS BIG BUSINESS

Identity theft is big business these days and law enforcement officials are engaged in a coordinated effort to stop it.
<http://www.net-security.org/news.php?id=4398>

KAZAA DELIVERS MORE THAN TUNES

Forty-five percent of the executable files downloaded through Kazaa, the most popular file-sharing program, contain malicious code like viruses and Trojan horses, according to a new study.
<http://www.net-security.org/news.php?id=4400>

FLAWS THREATEN VOIP NETWORKS

A technical review conducted by the British government has found several security flaws in products that use VoIP and

text messaging, including those from Microsoft and Cisco Systems.
<http://www.net-security.org/news.php?id=4401>

WIRELESS LAN SECURITY WORRIES ON HORIZON

This is supposed to be the year that the wireless industry addresses serious security shortcomings that are holding back enterprise wireless LAN rollouts.

<http://www.net-security.org/news.php?id=4402>

NO RELIEF FROM MICROSOFT PHISHING BUG

Redmond fails to patch a bug in Internet Explorer that makes consumers easy prey for online fraudsters.

<http://www.net-security.org/news.php?id=4403>

TELECOMS, ISPS PARTNER IN SPAM FIGHT

A group of international telecom providers, Internet service providers and software companies plan to form a "neighborhood watch" to oust junk e-mail from their collective networks, in what is the latest industry coalition bent on eradicating spam.

<http://www.net-security.org/news.php?id=4404>

RESEARCHER FOR WHOM EXPLOIT CODE MEANS FREEDOM OF SPEECH

Georgi Guninski is a man who is respected on vulnerability mailing lists. The Bulgarian security expert - and this is one instance when the word can be safely used - has spread himself wide when it comes to security but all of his vulnerability posts merit attention.

<http://www.net-security.org/news.php?id=4405>

USE PKI TO BEAT PHISHERS

Digital certificates could ward against internet scams.

<http://www.net-security.org/news.php?id=4406>

3COM RELEASES SUPER-SWITCH WITH BUILT-IN SECURITY

3Com has announced the immediate availability of a new super-switch that combines your normal switch with a firewall, anti-virus, content filtering and intrusion detection - in short, a network's security all in one box.

<http://www.net-security.org/news.php?id=4407>

BROWSER SECURITY TAKES OFF IN VPNS

Corporations are embracing a simpler, cheaper way of connecting remote workers to their networks, opening up new opportunities and competition--for network security vendors.

<http://www.net-security.org/news.php?id=4408>

NEW ANTI-SPAM LAWS FAIL TO BITE

E-mail users on both sides of the Atlantic hoping for a legislative

reprieve from spam are feeling let down.
<http://www.net-security.org/news.php?id=4409>

NOVELL TARGETS WEB SERVICES SECURITY

Novell is integrating its identity management and Web services software in a way that it says will ease customers' ability to secure corporate networks.
<http://www.net-security.org/news.php?id=4410>

PROBLEMS AND CHALLENGES WITH HONEYPOTS

For the past 18 months we have seen a tremendous growth in honeypot technologies.
<http://www.net-security.org/news.php?id=4411>

CORPORATE DATA FLIES OUT THE WINDOWS

Steve Bale, chief executive officer of ArmourSoft, examines the disadvantages for the enterprise of the legacy of Microsoft's personal computing origins.
<http://www.net-security.org/news.php?id=4412>

STANDARDIZING ON SECURITY

The Linux standards group publishes 565 pages of data describing a standards-compliant Linux package. So why aren't any of them about security?
<http://www.net-security.org/news.php?id=4413>

SECURITY FIRMS PUT UP 'PERSONAL FIREWALL DAY'

Straddling the line between public service and marketing, Microsoft and a handful of security companies are sponsoring a campaign to heighten consumer security awareness and have declared Jan. 15 "Personal Firewall Day."
<http://www.net-security.org/news.php?id=4414>

USER SEES SOME RESULT FROM MICROSOFT SECURITY FOCUS

Users appear resigned to patching software ad nauseam, though one large user welcomes Microsoft Corp.'s latest attempts to ease the pain of implementing fixes.
<http://www.net-security.org/news.php?id=4416>

IS SSL SECURITY OVER-HYPED?

Vendors were fast to back SSL-based virtual private networks, but are they really better than IPSec alternatives?
<http://www.net-security.org/news.php?id=4417>

PAYPAL SCAM TRIES TO JUMPSTART MIMAIL WORM

After releasing a version of the Mimail e-mail worm last week, virus authors are using a tool this week to help it spread: spam e-mail containing a Trojan horse program that, once

installed, retrieves and installs the worm.
<http://www.net-security.org/news.php?id=4418>

WHO'S PATCHING OPEN SOURCE?

In one of the great ironies of the software industry, Covalent's management software -- though known for open-source management -- is a proprietary product. Unlike most of the programs it manages, the CAM software code is not transparent or changeable by those who use it.

<http://www.net-security.org/news.php?id=4419>

TRACKING THE SEEDS OF DESTRUCTION

In studying the effects of last summer's MSBlast worm, some security experts turned to an unlikely source in search of clues to the prevention of computer epidemics: plants.

<http://www.net-security.org/news.php?id=4420>

GAO FAULTS 'INCONSISTENT' ONLINE SECURITY PROGRAMS

Spending amounting to \$1 billion has resulted in decidedly mixed results for public key infrastructure projects.

<http://www.net-security.org/news.php?id=4421>

REMOTE WORKING HEIGHTENS SECURITY

The advance of SSL has boosted corporate adoption of VPNs.

<http://www.net-security.org/news.php?id=4422>

SPAM WITH TROJAN HORSE ATTACKS EBAY USERS

Virus authors are using spam e-mails containing a Trojan horse program to help spread the latest version of the Mmail e-mail worm.

<http://www.net-security.org/news.php?id=4424>

[**Vulnerabilities**]

All vulnerabilities are located here:

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

RapidCache Multiple Vulnerabilities

<http://www.net-security.org/vuln.php?id=3184>

Symantec LiveUpdate Privilege Escalation Vulnerability
<http://www.net-security.org/vuln.php?id=3183>

Phpdig 1.6.X Remote Command Execution Vulnerability
<http://www.net-security.org/vuln.php?id=3182>

WWW Fileshare Pro Multiple Vulnerabilities
<http://www.net-security.org/vuln.php?id=3181>

Windows FTP Server Format String Vulnerability
<http://www.net-security.org/vuln.php?id=3180>

PHP Manpage Lookup Multiple Vulnerabilities
<http://www.net-security.org/vuln.php?id=3179>

ezContents Remote Code Execution Vulnerability
<http://www.net-security.org/vuln.php?id=3178>

Accipiter Direct Server 6.0 Directory Traversal Vulnerability
<http://www.net-security.org/vuln.php?id=3177>

[**Advisories**]

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

OpenPKG Security Advisory - tcpdump (OpenPKG-SA-2004.002)
<http://www.net-security.org/advisory.php?id=2895>

Trustix Secure Linux Security Advisory - tcpdump
(2004-0004 revision)
<http://www.net-security.org/advisory.php?id=2894>

Trustix Secure Linux Security Advisory - tcpdump (2004-0004)
<http://www.net-security.org/advisory.php?id=2893>

SUSE Security Announcement - Linux Kernel (x86_64, AMD64)
(SuSE-SA:2004:003)
<http://www.net-security.org/advisory.php?id=2892>

nCipher Security Advisory No. 8 - payShield library may
verify bad requests
<http://www.net-security.org/advisory.php?id=2891>

CERT Advisory CA-2004-01 -Multiple H.323 Message Vulnerabilities
<http://www.net-security.org/advisory.php?id=2890>

KDE Security Advisory: VCF file information reader vulnerability
(2004-01-14)
<http://www.net-security.org/advisory.php?id=2889>

SmoothWall Project Security Advisory - Updates for SmoothWall
Express to correct local vulnerabilities in Linux kernel
(SWP-2004:001)
<http://www.net-security.org/advisory.php?id=2888>

Debian Security Advisory - New Linux 2.4.17 packages
fix several problems (ia64) (DSA 423-1)
<http://www.net-security.org/advisory.php?id=2887>

Slackware Security Advisory - INN security update (SSA:2004-014-02)
<http://www.net-security.org/advisory.php?id=2886>

Slackware Security Advisory - kdepim security update
(SSA:2004-014-01)
<http://www.net-security.org/advisory.php?id=2885>

Mandrake Linux Security Update Advisory - kdepim (MDKSA-2004:003)
<http://www.net-security.org/advisory.php?id=2884>

Red Hat Security Advisory - Updated tcpdump packages
fix various vulnerabilities (RHSA-2004:007-01)
<http://www.net-security.org/advisory.php?id=2883>

HP Security Bulletin - Tru64 UNIX potential Denial of Service
and/or unauthorized access (SSRT3629A/B)
<http://www.net-security.org/advisory.php?id=2882>

SUSE Security Announcement - tcpdump (SuSE-SA:2004:002)
<http://www.net-security.org/advisory.php?id=2881>

Red Hat Security Advisory - Updated kdeim packages
resolve security vulnerability (RHSA-2004:006-01)
<http://www.net-security.org/advisory.php?id=2880>

Cisco Security Advisory - Vulnerabilities in H.323 Message
Processing (47843)
<http://www.net-security.org/advisory.php?id=2879>

Mandrake Linux Security Update Advisory - ethereal (MDKSA-2004:002)
<http://www.net-security.org/advisory.php?id=2878>

HP Security Bulletin - Tru64 UNIX potential Denial of Service
and/or unauthorized access (SSRT3629A/B)
<http://www.net-security.org/advisory.php?id=2877>

Microsoft Exchange Server Security Bulletin Summary for January 2004
<http://www.net-security.org/advisory.php?id=2876>

Microsoft ISA Server Security Bulletin Summary for January 2004
<http://www.net-security.org/advisory.php?id=2875>

Microsoft Windows Security Bulletin Summary for January 2004
<http://www.net-security.org/advisory.php?id=2874>

Microsoft Security Updates Alert - January 2003
<http://www.net-security.org/advisory.php?id=2873>

Debian Security Advisory - multiple CVS improvements (DSA-422-1)
<http://www.net-security.org/advisory.php?id=2872>

Debian Security Advisory - New mod-auth-shadow packages
fix password expiration checking (DSA 421-1)
<http://www.net-security.org/advisory.php?id=2871>

Red Hat Security Advisory - Updated CVS packages fix minor
security issue (RHSA-2004:003-01)
<http://www.net-security.org/advisory.php?id=2870>

Conectiva Linux Security Announcement - ethereal (CLA-2004:801)
<http://www.net-security.org/advisory.php?id=2869>

Debian Security Advisory - New jitterbug packages fix
arbitrary command execution (DSA 420-1)
<http://www.net-security.org/advisory.php?id=2868>

[Articles]

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

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

FREEBSD 5.2 IS HERE

This release contains a number of significant stability and performance improvements over FreeBSD 5.1. Read on to find out what security issues have been fixed in this version.
<http://www.net-security.org/article.php?id=627>

THE CORPORATE IDENTITY CRISIS

Secure messaging has traditionally posed a problem in a corporate environment for two main reasons: firstly, the complexity of maintaining the infrastructure of "keys," which serve similar roles to unique identification credentials, and secondly, the complexity of explaining and using the solutions.
<http://www.net-security.org/article.php?id=628>

[Reviews]

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

BEGINNING RED HAT LINUX 9

The many authors managed to squeeze into this title the most important facts for a novice user and point him into the right direction. Read on to discover what's inside this book.
<http://www.net-security.org/review.php?id=120>

IMPLEMENTING SSH: STRATEGIES FOR OPTIMIZING THE SECURE SHELL

With a bunch of security features, SSH is being adopted by a great number of system administrators that are trying to implement some way of secure tunneling to their networks. Although the title of the book implies a very technical publication, the book should suite a variety of readers interested in how to use and optimize the secure shell.
<http://www.net-security.org/review.php?id=121>

[**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

AET TRACER PRO 3.01

AET Tracer Pro is a network tool collection. The collection includes: geographical positioning, trace route, IP tracer, e-mail tracer, interactive Netstat GUI, automated Whois GUI, automated abuse reporter and a network scanner with seven different scan methods.

<http://www.net-security.org/software.php?id=536>

[**Webcasts**]

All webcasts are located at:

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

Monthly Update from Microsoft's VP for Security
Organized by Microsoft on 20 January 2004, 8:30 AM PT
<http://www.net-security.org/webcast.php?id=151>

Monthly Update from Microsoft's VP for Security
Organized by Microsoft on 20 January 2004, 8:30 AM
<http://www.net-security.org/webcast.php?id=167>

Tripwire for Servers: Overview and Product Demo
Organized by Tripwire on 20 January 2004, 11:00 AM PDT
<http://www.net-security.org/webcast.php?id=178>

The Basics of WLAN Security
Organized by Funk Software on 20 January 2004, 1:00 PM EST
<http://www.net-security.org/webcast.php?id=156>

Designing a Secure - Reliable - and Usable Patch Management Infrastructure

Organized by Microsoft on 21 January 2004, 11:30 AM PT
<http://www.net-security.org/webcast.php?id=168>

Penetration Testing with CORE IMPACT

Organized by Core Security Technologies on 21 January 2004, 2:00 PM et
<http://www.net-security.org/webcast.php?id=180>

Tripwire for Network Devices: Overview and Product Demo

Organized by Tripwire on 22 January 2004, 11:00 AM PDT
<http://www.net-security.org/webcast.php?id=175>

Best ASP.NET Practices for Shielding Your Site from Hackers

Organized by Microsoft on 22 January 2004, 1:00 PM PT
<http://www.net-security.org/webcast.php?id=169>

Best Practices: Taking Proactive Measures Before The Next Exploit

Organized by eEye on 22 January 2004, 2:00 PM PST
<http://www.net-security.org/webcast.php?id=149>

Web Application Security: Enforcing Security Management & Compliance

Organized by Symantec on 22 January 2004, 2:00 PM EST
<http://www.net-security.org/webcast.php?id=182>

Essentials of Security

Organized by Microsoft on 23 January 2004, 9:30 AM PT
<http://www.net-security.org/webcast.php?id=170>

Tripwire for Network Devices: Overview and Product Demo

Organized by Tripwire on 27 January 2004, 11:00 AM PDT
<http://www.net-security.org/webcast.php?id=176>

ASP.NET Security Best Practices

Organized by Microsoft on 28 January 2004, 9:00 AM PT
<http://www.net-security.org/webcast.php?id=172>

Implementing Client Security on Windows 2000 and Windows XP

Organized by Microsoft on 28 January 2004, 1:00 PM PT
<http://www.net-security.org/webcast.php?id=171>

[Conferences]

All conferences are located at:

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

Security Venture Fair

Organized by Infocast - 21 January-23 January 2004

<http://www.net-security.org/conference.php?id=78>

IT-Defense 2004

Organized by cirosec GmbH/dpunkt.Verlag - 28 January -
30 January 2004

<http://www.net-security.org/conference.php?id=56>

FAA IT/ISS Partnership Conference

Organized by FBC - 10 February-11 February 2004

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

Infosecurity Italia 2004

Organized by Fiera Milano International - 13 February -
14 February 2004

<http://www.net-security.org/conference.php?id=34>

RSA Conference 2004 USA

Organized by RSA Security - 23 February-27 February 2004

<http://www.net-security.org/conference.php?id=55>

Southeast Cybercrime Summit 2004

Organized by ATLCCS - 2 March-5 March 2004

<http://www.net-security.org/conference.php?id=77>

InfoSec World Conference and Expo 2004

Organized by MIS Training Institute - 22 March-24 March 2004

<http://www.net-security.org/conference.php?id=68>

Infosecurity Europe 2004

Organized by Reed Exhibitions - 27 April-29 April 2004

<http://www.net-security.org/conference.php?id=27>

Dallascon Security Conference 2004

Organized by DallasCon - 1 May-2 May 2004

<http://www.net-security.org/conference.php?id=73>

RSA Conference 2004 Japan
Organized by RSA Conference 2004 Japan Executive
Committee - 31 May-1 June 2004
<http://www.net-security.org/conference.php?id=82>

BCS Birmingham IT Security Conference 2004
Organized by British Computer Society - 8 June-8 June 2004
<http://www.net-security.org/conference.php?id=81>

16th Annual FIRST Conference
Organized by FIRST - 13 June-18 June 2004
<http://www.net-security.org/conference.php?id=22>

NetSec 2004
Organized by Computer Security Institute - 14 June-16 June 2004
<http://www.net-security.org/conference.php?id=20>

2004 USENIX Annual Technical Conference
Organized by USENIX Association - 27 June-2 July 2004
<http://www.net-security.org/conference.php?id=66>

DIMVA 2004
Organized by German Informatics Society - 6 July-7 July 2004
<http://www.net-security.org/conference.php?id=47>

[**Security world**]

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

Send your press releases to press@net-security.org

NetScreen SSL VPN Appliances Named Security Technologies
Product of the Year by Frost & Sullivan
<http://www.net-security.org/press.php?id=1921>

New Alcatel Enterprise Network Management Applications
Save Network Administration Time and Ensure Secure Management
<http://www.net-security.org/press.php?id=1920>

Panda Software Warns of Fraudulent Bank E-Mails
<http://www.net-security.org/press.php?id=1919>

Cyberguard's Snapgear Announces Major Upgrade to
VPN/Firewall Appliance With Intrusion Detection System
<http://www.net-security.org/press.php?id=1918>

Internet Security Systems Acquires Content Security
Pioneer Cobion
<http://www.net-security.org/press.php?id=1917>

Vontu Announces Industry's First Data Firewall to Battle
Insider Information Leakage and Identity Theft
<http://www.net-security.org/press.php?id=1916>

Advanced Document Filtering And Enhanced Policy Management
Capabilities Are a Win For Sharepoint Users
<http://www.net-security.org/press.php?id=1915>

SSH Receives Fips 140-2 Certification
<http://www.net-security.org/press.php?id=1914>

Nissho Electronics And Netcontinuum Partner to Bring Web
Application Security and DMZ Efficiency To Japanese Market
<http://www.net-security.org/press.php?id=1913>

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

FREE GUIDE-128-bit encryption

Thawte is one of the few companies that offers 128 bit supercerts.
A supercert will allow you to extend the highest allowed 128 bit
encryption to all your clients even if they use browsers that are
limited to 40 bit encryption.

Download a guide to learn more.
<http://ad.doubleclick.net/clk;6091071;8369141;h>
