



HNS Newsletter

Issue 219 - 28.06.2004.

<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.

ADVERTISEMENT

Windows Server System is integrated server infrastructure software from Microsoft that is designed to work together and interact seamlessly with other data and applications across your IT environment so you can reduce the costs of ongoing operations, deliver highly reliable and secure IT infrastructure, and drive valuable new capabilities for the future growth of your business.

For more information visit:

<http://ad.sk.doubleclick.net/clk;8032547;9084238;o>

Table of contents:

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

[Security news]

US MOVES TOWARDS ANTI-SPYWARE LAW

A US House subcommittee on Thursday (17 May) approved what would be the first federal law to specifically target Internet spyware.

<http://www.net-security.org/news.php?id=5442>

EXPERTS WORRY ABOUT TECH RETALIATION

A Texas company wants to bring vigilante justice to cyberspace.

<http://www.net-security.org/news.php?id=5443>

STEALTH WALLPAPER COULD KEEP WLANS SECURE

Keeps outsiders off your wired or wireless network.

<http://www.net-security.org/news.php?id=5444>

FEDS FACE NUMEROUS ENCRYPTION SCHEMES FOR SECURING E-MAIL

Government agencies face a communications dilemma. On one hand, officials are asked to share more information with other agencies, businesses and citizens.

<http://www.net-security.org/news.php?id=5446>

SENATE DEBATES CYBERCRIME TREATY

A controversial treaty that is the first to focus on computer crime is inching toward ratification in the U.S. Senate.

<http://www.net-security.org/news.php?id=5447>

NEW GADGETS TAKE ON 'STARBUCKS' SECURITY THREAT

Two companies offer plug-in devices that secure info, communications over wireless networks.

<http://www.net-security.org/news.php?id=5448>

CISCO RAISING ROUTER SECURITY

Cisco will announce availability of its Network Admission Control security technology for Cisco routers this week and lay out a road map for adding NAC capabilities to its lines of LAN switches.

<http://www.net-security.org/news.php?id=5449>

OUTLOOK'S SECURITY COMPROMISED BY SPAMMERS

Spammers have found a way to bypass Outlook 2003's anti-spam security by embedding images into their emails.

<http://www.net-security.org/news.php?id=5450>

HANDY WIRELESS NETWORKING WITH KNOPPIX LINUX

Few LiveCD distros come configured with support for the Linksys WPC55AG adapter, which requires the MadWiFi modules with a correctly configured kernel.

<http://www.net-security.org/news.php?id=5451>

GADGETS SECURE PCS ON PUBLIC WI-FI

Seclarity of San Francisco is introducing this week its SiNic Wireless network interface card.

<http://www.net-security.org/news.php?id=5452>

MICROSOFT SECURITY FLAW MODERATE THIS MONTH

Microsoft Corp. recently issued a security update for a 'Denial of Service' vulnerability that exists in the IDirectPlay4 application programming interface (API) of its DirectPlay, according to a statement on the company's website.

<http://www.net-security.org/news.php?id=5453>

NETWORK ASSOCIATES UP FOR SALE, SOURCES SAY

Network Associates is for sale, and Microsoft is rumored to be the buyer.

<http://www.net-security.org/news.php?id=5454>

FOREMOST: A LINUX COMPUTER FORENSICS TOOL

Computer sleuths interested in running forensic PC operations on a Linux machines should take a look at an open source tool called Foremost.

<http://www.net-security.org/news.php?id=5455>

HNS AUDIO LEARNING SESSION: THE BENEFITS OF SSL VPNS

Rob Lane, AEP Systems VP of Product Management, discusses SSL VPNs in general, shares his point of view on the benefits of using SSL VPNs for secure remote access and talks about the difference between SSL and IPsec VPNs.

<http://www.net-security.org/news.php?id=5456>

NETWORK ASSOCIATES DENIES SALE RUMORS

Security company Network Associates said Tuesday that there's no truth to rumors that it is considering an offer to be bought by a large company, possibly Microsoft.

<http://www.net-security.org/news.php?id=5457>

FOUR CRITERIA FOR EVALUATING A SECURITY VENDOR

When evaluating security products for your enterprise, make sure you also evaluate the vendors themselves using these criteria.

<http://www.net-security.org/news.php?id=5458>

WI-FI SECURITY STANDARD NEARS APPROVAL

Industry sources said the IEEE 802.11i specification could be ratified this Thursday, adding a needed layer of security to the Wi-Fi standard.

<http://www.net-security.org/news.php?id=5459>

NETWORK ADMINS GET PEEK AT MICROSOFT'S SECURITY

Microsoft's top network security manager appeared at a company road show Tuesday to let other administrators know what the software giant is doing to help keep corporate networks safe.

<http://www.net-security.org/news.php?id=5460>

BLIND GET EARFUL OF SPAM DAILY

It's annoying to read spam. It's even worse to hear it. Blind users rely on text-to-speech programs to hear what's on their screens, and they face an aural assault daily.

<http://www.net-security.org/news.php?id=5461>

WINDOWS XP SP2 CAN BREAK THINGS

Learn about the plethora of security enhancements that Microsoft has included in Windows XP Service Pack 2, as well as how these security features could impair the functionality of some applications.

<http://www.net-security.org/news.php?id=5462>

MICROSOFT, AOL, YAHOO UNVEIL ANTISPAM GUIDELINES

An industry organization representing heavyweight e-mail providers Yahoo Inc., Microsoft Corp., America Online Inc. and EarthLink Inc. released recommendations for ending unsolicited commercial ("spam") e-mail, according to a statement by the group.

<http://www.net-security.org/news.php?id=5463>

IM WORMS COULD SPREAD IN SECONDS

Using public IM networks poses some special problems for enterprises.

<http://www.net-security.org/news.php?id=5464>

US ROBOTICS ON THE ROUTE TO IMPROVED SECURITY

US Robotics has launched a new router, which offers a plethora of security features and what the firm claims are unique file server capabilities.

<http://www.net-security.org/news.php?id=5466>

MASTERCARD TACKLES PHISHING

Credit card giant MasterCard announced on Tuesday a new initiative aimed at fighting the growing problem of online fraud, specifically the emerging threat of "phishing" schemes.

<http://www.net-security.org/news.php?id=5467>

TIPS FOR REMOVING SPYWARE FROM YOUR PC

Has your PC been sluggish lately, with a lot more pop-up ads? It could be spyware.

<http://www.net-security.org/news.php?id=5468>

AOL ENGINEER SOLD 92 MILLION SCREEN NAMES TO SPAMMER

Jason Smathers, an America Online engineer, has been arrested and charged with stealing tens of millions of AOL screen names and then selling them to several people.

<http://www.net-security.org/news.php?id=5469>

WI-FI GETS MUCH-NEEDED SECURITY BOOST

A Wi-Fi security standard awaiting final approval is intended to

restore confidence in a market damaged by previous weak specifications.

<http://www.net-security.org/news.php?id=5470>

BUGWATCH: REDUCING DOWNTIME AT THE DATA CENTRE

Paul Smith, UK country manager with KVM switching and connectivity company Avocent, considers how to minimise potential physical security threats to data servers.

<http://www.net-security.org/news.php?id=5471>

WHEN SPYWARE CROSSES THE LINE

Kelly Martin is the content editor for SecurityFocus, gives her opinion on malicious "spyware" applications.

<http://www.net-security.org/news.php?id=5472>

ETHICAL HACKING IS NO OXYMORON

Sporting long sideburns, a bushy goatee and black baseball cap, instructor Ralph Echemendia has a class of 15 buttoned-down corporate, academic and military leaders spellbound. The lesson: hacking.

<http://www.net-security.org/news.php?id=5473>

OASIS APPROVES SECURITY SPEC FOR APPS, WEB SERVICES

To help companies better handle the influx of application and Web service security alerts, the OASIS standards consortium on Wednesday announced the ratification of a new standard.

<http://www.net-security.org/news.php?id=5474>

HOW TO USE CRYPTOGRAPHY IN COMPUTER SECURITY

Cryptography is the mathematics underlying computer security. While a Ph.D. in cryptography is hardly a requirement for keeping one's systems secure, an understanding of the basics helps in decision making about security, both for system administrators and IT managers.

<http://www.net-security.org/news.php?id=5475>

MAC OS X SECURITY MYTH EXPOSED

Windows is more secure than you think, and Mac OS X is worse than you ever imagined. That is according to statistics published for the first time this week by Danish security firm Secunia.

<http://www.net-security.org/news.php?id=5476>

SECURITY BREACHES, CONGESTION FOUND AT TRADE SHOW WLAN

Attendees of this week's Supercomm trade show in Chicago faced a variety of wireless LAN security breaches, according to a firm that specializes in wireless security.

<http://www.net-security.org/news.php?id=5477>

INTERVIEW WITH GENE HODGES, NETWORK ASSOCIATES PRESIDENT

Before the latest wave of speculation about the potential sale of Network Associates, company President Gene Hodges discussed the security software vendor's future and the current security market with CRN Editor in Chief Michael Vizard.

<http://www.net-security.org/news.php?id=5478>

COULD SEARCH SITES SPAWN WORMS?

Worm attacks are bad enough by themselves, but some experts warn of an even more devastating variation: one that strikes at the application level instead of targeting network infrastructure, and spreads to Web sites through Web-based search engines.

<http://www.net-security.org/news.php?id=5479>

COOKIE PATH BEST PRACTICE

Cookies are often used to maintain a Session ID (SID), through which an individual user can be identified throughout their interaction with the site. If an attacker can use a mechanism to gain access to the SID, then potentially they can incorporate it within their own session to successfully assume the users identity.

<http://www.net-security.org/news.php?id=5480>

[**Vulnerabilities**]

All vulnerabilities are located here:

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

FreeBSD Local Denial of Service Vulnerability

<http://www.net-security.org/vuln.php?id=3531>

Gnats Format String Vulnerability

<http://www.net-security.org/vuln.php?id=3530>

Artmedic_links5 File Include Vulnerability

<http://www.net-security.org/vuln.php?id=3529>

Drcatd Multiple Vulnerabilities

<http://www.net-security.org/vuln.php?id=3528>

rlprd 2.0.4 Format String Vulnerability
<http://www.net-security.org/vuln.php?id=3527>

vBulletin HTML Injection Vulnerability
<http://www.net-security.org/vuln.php?id=3526>

Linux Broadcom 5820 Cryptonet Driver Integer Overflow Vulnerability
<http://www.net-security.org/vuln.php?id=3525>

BT Voyager 2000 Wireless ADSL Router Cleartext Password Vulnerability
<http://www.net-security.org/vuln.php?id=3524>

Sqwebmail 4.0.4 Cross Site Scripting Vulnerability
<http://www.net-security.org/vuln.php?id=3523>

Internet Explorer HTML Printing Denial of Service Vulnerability
<http://www.net-security.org/vuln.php?id=3522>

ArbitroWeb v0.6 Javascript Injection Vulnerability
<http://www.net-security.org/vuln.php?id=3521>

Lotus Notes URI Handler Argument Injection Vulnerability
<http://www.net-security.org/vuln.php?id=3519>

DLink 704 Script Injection Vulnerability
<http://www.net-security.org/vuln.php?id=3518>

DLink 614+ Script Injection Vulnerability
<http://www.net-security.org/vuln.php?id=3517>

ZoneAlarm Pro 'Mobile Code' Bypass Vulnerability
<http://www.net-security.org/vuln.php?id=3516>

Netgear FVS318 Web-Based Administration Denial of Service
Vulnerability
<http://www.net-security.org/vuln.php?id=3515>

Microsoft MN-500 Wireless Router Web-Based Administration Denial of
Service Vulnerability
<http://www.net-security.org/vuln.php?id=3514>

Internet Scanner 7 Restriction Bypass Vulnerability
<http://www.net-security.org/vuln.php?id=3513>

DNSONE Appliance Script Injection Vulnerability
<http://www.net-security.org/vuln.php?id=3512>

"IBM Access Support" (eGatherer) Activex Dangerous Methods
Vulnerability
<http://www.net-security.org/vuln.php?id=3511>

[**Advisories**]

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

Debian Security Advisory - New apache packages fix buffer overflow in
mod_proxy (DSA 525-1)
<http://www.net-security.org/advisory.php?id=3485>

Gentoo Linux Security Advisory - FreeS/WAN, Openswan, strongSwan:
Vulnerabilities in certificate handling (GLSA 200406-20)
<http://www.net-security.org/advisory.php?id=3484>

Gentoo Linux Security Advisory - gzip: Insecure creation of temporary
files (GLSA 200406-18)
<http://www.net-security.org/advisory.php?id=3483>

Gentoo Linux Security Advisory - giFT-FastTrack: remote denial of
service attack (GLSA 200406-19)
<http://www.net-security.org/advisory.php?id=3482>

Mandrakelinux Security Update Advisory - kernel (MDKSA-2004:062)
<http://www.net-security.org/advisory.php?id=3481>

SUSE Security Announcement - dhcp-server (SuSE-SA:2004:019)
<http://www.net-security.org/advisory.php?id=3480>

US-CERT Technical Cyber Security Alert TA04-174A -- Multiple
Vulnerabilities in ISC DHCP 3
<http://www.net-security.org/advisory.php?id=3479>

Gentoo Linux Security Advisory - IPsec-Tools: authentication bug in racoon (GLSA 200406-17)
<http://www.net-security.org/advisory.php?id=3478>

Conectiva Security Announcement - kernel (CLA-2004:845)
<http://www.net-security.org/advisory.php?id=3477>

SGI Security Advisory - SGI Advanced Linux Environment 2.4 security update #22 (20040605-01-U)
<http://www.net-security.org/advisory.php?id=3476>

SGI Security Advisory - SGI Advanced Linux Environment 3 Security Update #4 (20040604-01-U)
<http://www.net-security.org/advisory.php?id=3475>

Gentoo Linux Security Advisory - Apache 1.3: Buffer overflow in mod_proxy (GLSA 200406-16)
<http://www.net-security.org/advisory.php?id=3474>

SGI Security Advisory - SGI Advanced Linux Environment 3 Security Update #3 (20040603-01-U)
<http://www.net-security.org/advisory.php?id=3473>

SGI Security Advisory - SGI Advanced Linux Environment 2.4 security update #21 (20040602-01-U)
<http://www.net-security.org/advisory.php?id=3472>

Guardian Digital Security Advisory - 'kernel' Several vulnerabilities (ESA-20040621-005)
<http://www.net-security.org/advisory.php?id=3471>

Debian Security Advisory - New rlpr packages fix multiple vulnerabilities (DSA 524-1)
<http://www.net-security.org/advisory.php?id=3470>

Debian Security Advisory - New www-sql packages fix buffer overflow (DSA 523-1)
<http://www.net-security.org/advisory.php?id=3469>

Debian Security Advisory - New super packages fix format string vulnerability (DSA 522-1)
<http://www.net-security.org/advisory.php?id=3468>

Debian Security Advisory - New sup packages fix format string vulnerabilities (DSA 521-1)
<http://www.net-security.org/advisory.php?id=3467>

Gentoo Linux Security Advisory - Usermin: Multiple vulnerabilities (GLSA 200406-15)
<http://www.net-security.org/advisory.php?id=3466>

Trustix Secure Linux Security Advisory - kernel (#2004-0035)
<http://www.net-security.org/advisory.php?id=3465>

Turbolinux Security Announcement - kernel crash (18/Jun/2004)
<http://www.net-security.org/advisory.php?id=3464>

[Articles]

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

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

COOKIE PATH BEST PRACTICE

Cookies provide a method for creating a stateful HTTP session. They are often used to maintain a Session ID (SID), through which an individual user can be identified throughout their interaction with the site. If an attacker can use a mechanism (such as sniffing or cross site scripting) to gain access to the SID, then potentially they can incorporate it within their own session to successfully assume the users identity.

<http://www.net-security.org/article.php?id=704>

HNS AUDIO LEARNING SESSION: THE BENEFITS OF SSL VPNS

In this HNS audio learning session, Rob Lane, AEP Systems VP of Product Management, discusses about SSL VPNs in general, shares his point of view on the benefits of using SSL VPNs for secure remote access and talks about the difference between SSL and IPSec VPNs.

<http://www.net-security.org/article.php?id=703>

SECURE DEVELOPMENT FRAMEWORK

This whitepaper focuses on why a secure development framework is needed, touches on its benefits and provides an overview of how organisations can implement such strategies successfully. A simple

software development model is used as an example in the paper, but the theories are expected to be developed and adapted to suit the specific methodologies and goals of any environment.
<http://www.net-security.org/article.php?id=702>

[Reviews]

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

HACKNOTES NETWORK SECURITY PORTABLE REFERENCE

This book is perfectly suited for two different types of readers: those who are working within the Information Security field and need to catch up with some of the most common security issues and procedures, and for those who need to show their upper management the magnitude of possible security risks in a network environment.

<http://www.net-security.org/review.php?id=132>

[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

Pocket PC software is located at:
http://net-security.org/software_main.php?cat=3

EASY INTEGRITY CHECK SYSTEM 3.1

Easy integrity check system is designed primarily for system administrators for filesystem integrity checkings.
<http://www.net-security.org/software.php?id=410>

LOGWATCH 5.2.1

Logwatch is a customizable log analysis system.
<http://www.net-security.org/software.php?id=129>

MARADNS 1.1.21

MaraDNS is a DNS server that strives to be secure and fully open-sourced.
<http://www.net-security.org/software.php?id=84>

OS-SIM 0.9.5p2

OSSIM is a distribution of open source products that are integrated to provide an infrastructure for security monitoring.
<http://www.net-security.org/software.php?id=304>

ROOTKIT HUNTER 1.1.1

Rootkit scanner is scanning tool to ensure you for about 99.9% you're clean of nasty tools.
<http://www.net-security.org/software.php?id=531>

SHOREWALL 2.0.3 RC2

Shorewall is an iptables based firewall that can be used on a dedicated firewall system, a multi-function masquerade gateway/server or on a standalone Linux system.
<http://www.net-security.org/software.php?id=40>

[**Webcasts**]

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

Securing the Development Process
Organized by Microsoft on 29 June 2004, 11:00 AM
<http://www.net-security.org/webcast.php?id=301>

All anti-virus software is not created equal
Organized by Sophos on 30 June 2004, 10:00 AM
<http://www.net-security.org/webcast.php?id=286>

Developing a Software Security Metrics Program
Organized by Foundstone on 14 July 2004, 4:00 PM
<http://www.net-security.org/webcast.php?id=294>

[Conferences]

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

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

Security Leadership Council 2004
Organized by IP Events, Inc. - 29 June-30 June 2004
<http://www.net-security.org/conference.php?id=92>

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

RUXCON 2004
Organized by Australian computer security community - 10 July-11 July 2004
<http://www.net-security.org/conference.php?id=88>

Open Source Convention 2004
Organized by O'Reilly - 26 July-30 July 2004
<http://www.net-security.org/conference.php?id=89>

13th USENIX Security Symposium
Organized by USENIX Association - 9 August-13 August 2004
<http://www.net-security.org/conference.php?id=67>

The 14th Virus Bulletin International Conference (VB2004)
Organized by Virus Bulletin - 29 September-1 October 2004
<http://www.net-security.org/conference.php?id=83>

RSA Conference Europe 2004
Organized by RSA Security - 3 November-5 November 2004
<http://www.net-security.org/conference.php?id=90>

IBM SecureWorld Conference EMEA 2004
Organized by IBM - 23 November-26 November 2004
<http://www.net-security.org/conference.php?id=91>

[**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

Introducing RoadBLOCK Security Firewall - An Advanced Intelligent
Network Security Appliance for the 21st Century
<http://www.net-security.org/press.php?id=2248>

Analysis of Web Site Penetration Retests Show 93% of Applications
Remain Vulnerable After "Fixes"
<http://www.net-security.org/press.php?id=2247>

(ISC)2 CISSP Security Credential Achieves New International Standard
For Personnel Certification
<http://www.net-security.org/press.php?id=2246>

Sophos Named Frost & Sullivan's European Security Company Of The Year
<http://www.net-security.org/press.php?id=2245>

The 1st Worldwide Internet Security Campaign Offers Anti-Dialer Tools
<http://www.net-security.org/press.php?id=2244>

C1 Secure eBusiness Extends its E-Mail Security Solution
<http://www.net-security.org/press.php?id=2243>

Kaspersky Labs Steps Forward with Linux - The Company Becomes a SUSE
Technology Partner
<http://www.net-security.org/press.php?id=2242>

TippingPoint Extends UnityOne Intrusion Prevention Systems to Block
Attacks Targeting VoIP
<http://www.net-security.org/press.php?id=2241>

Certicom Wins Frost and Sullivan Award for Excellence in Technology
<http://www.net-security.org/press.php?id=2240>

Sophos Protects Mac OS X Users From Virus Attack
<http://www.net-security.org/press.php?id=2239>

Panda Antivirus Gatedefender Protects the 6,500 Users at Santa Maria
Joint Union High School District
<http://www.net-security.org/press.php?id=2238>

ServGate Adds Edgeforce Web Filtering By Surfcontrol To Protect
Against Broadest Context Of Security Threats
<http://www.net-security.org/press.php?id=2237>

SAS Institute And SSH To Cooperate In IT Security Solutions
<http://www.net-security.org/press.php?id=2236>

Spyware Used By Spammers In New Twist On Spam Attacks
<http://www.net-security.org/press.php?id=2235>

Sanctum Achieves Certification in ICSA Labs' New Premier Services
Certification Program
<http://www.net-security.org/press.php?id=2234>

GFI Offers New GFI LANguard S.E.L.M. And GFI Network Server Monitor
Bundle
<http://www.net-security.org/press.php?id=2233>

Blue Coat Launches Proxyav Appliance For High-Performance Web
Anti-Virus
<http://www.net-security.org/press.php?id=2232>

TippingPoint's UnityOne Intrusion Prevention Systems Block 23 Million
Attacks at Stony Brook University
<http://www.net-security.org/press.php?id=2231>

BitDefender US Opens For Business New Office To Start Operations
Today
<http://www.net-security.org/press.php?id=2230>

Kaspersky Labs joins the Red Hat Ready Program
<http://www.net-security.org/press.php?id=2229>

Syngress Publishing Announces the Release of "Security Sage's Guide
to Hardening the Network Infrastructure"
<http://www.net-security.org/press.php?id=2228>

[**Virus News**]

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

Weekly Report on Viruses and Intrusions - Six Korgo variants,
Downloader.JH and IPScanner.A
http://www.net-security.org/virus_news.php?id=425

Weekly report on viruses and intrusions - Cabir, StartPage.FH,
Downloader.HC and Argen
http://www.net-security.org/virus_news.php?id=424

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

ADVERTISEMENT

Windows Server System is integrated server infrastructure
software from Microsoft that is designed to work together and
interact seamlessly with other data and applications across your
IT environment so you can reduce the costs of ongoing operations,
deliver highly reliable and secure IT infrastructure, and drive
valuable new capabilities for the future growth of your business.

For more information visit:
<http://ad.sk.doubleclick.net/clk;8032547;9084238;o>
