



HNS Newsletter
Issue 148 - 10.02.2003.
<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>.

*** **ALERT!** ***

ALL OF THE FOLLOWING APPLICATIONS ARE VULNERABLE TO ATTACK!:

*** Microsoft SQL Server
*** Lotus Domino
*** IBM DB2/UDB
*** Oracle
*** Sybase

Get a **FREE SAMPLE VULNERABILITY ASSESSMENT** of your DATABASE and APPLICATIONS from:

<http://www.appsecinc.com/helpnetsecurity/>

QUESTIONS: How Vulnerable are Your Applications and Databases? Are Your Databases Secured to Resist Another SQL Slammer/Sapphire Worm? Are You Confident Enough to Say That Your Applications and Databases Are Secure from Future Attacks?

ANSWER: Find out now and get a **FREE SAMPLE VULNERABILITY ASSESSMENT** of your DATABASE and APPLICATIONS from:

<http://www.appsecinc.com/helpnetsecurity/>

Table of contents:

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

[Security news]

SHOULD MICROSOFT PAY YOUR SECURITY PATCH COSTS?

The cost of keeping your network and systems secure should be a shared burden, not just a cost of doing business.

>> <http://www.net-security.org/news.php?id=1930>

MICROSOFT SECURITY GETS AN 'F'

"Trustworthy Computing is failing," Russ Cooper of TruSecure Corp. said of the Microsoft initiative. "I gave it a 'D-minus' at the beginning of the year, and now I'd give it an 'F.'"

>> <http://www.net-security.org/news.php?id=1931>

SLAMMER DIDN'T HURT, BUT THE NEXT ONE MIGHT

Agency says its air traffic control network wasn't compromised by worm's attack on the Internet, but admits it could happen in the future.

>> <http://www.net-security.org/news.php?id=1932>

TIGHTVNC: REMOTE X THE SECURE, FAST & EASY WAY

Looking for a software solution to help him access his home desktop remotely, Joe Barr finds more than he'd hoped for in TightVNC.

>> <http://www.net-security.org/news.php?id=1933>

MOBILE USERS FACE GROWING VIRUS THREAT

Virus writers are not yet targeting mobile platforms, but is this the calm before the storm?

>> <http://www.net-security.org/news.php?id=1934>

SOMETHING NEEDS TO CHANGE

With the Slammer worm network security becomes literally a matter of life and death. Where do we go from here?

>> <http://www.net-security.org/news.php?id=1935>

SECURE LINUX PREPARING FOR INDUSTRIAL CONTROL

A version of Linux hardened by the US Government is being proposed for industrial control systems.

>> <http://www.net-security.org/news.php?id=1936>

ESECURITY: TOWARDS A MORE SECURE INTERNET ENVIRONMENT

eSecurity is not only a concern in specialised areas such as aerospace, military applications and banking, but an issue for governments, businesses and consumers alike.

>> <http://www.net-security.org/news.php?id=1938>

WORM TURNS ON THE ARCHERS

The BBC has been hit by a virus for the second time in a month.

>> <http://www.net-security.org/news.php?id=1940>

SECURITY STRATEGIES: FORTRESS OR AIRPORT?

CIOs are scratching their heads, trying to figure out if they should adopt fortress-type security systems or move towards a multi layered security strategy.

>> <http://www.net-security.org/news.php?id=1941>

SECURING SYSTEMS WITH CHROOT

One popular technique crackers use to compromise machines is exploiting buffer overflows. Learn how to minimize the damage by using chroot.

>> <http://www.net-security.org/news.php?id=1942>

CYBER ATTACKS DOWN, BUT VULNS SOAR

The level of cyber attacks decreased for the first time in the second half of 2002, dropping six per cent.

>> <http://www.net-security.org/news.php?id=1943>

MITIGATING VOICE TELEPHONY SECURITY AND FRAUD RISKS

The trend toward the convergence of telephony and computer systems has exposed voice systems to abusers. IT executives should implement plans that will mitigate the chances of a hacker's success.

>> <http://www.net-security.org/news.php?id=1944>

SNOOPING STALLED

The U.S. House of Representatives and President Bush should concur with a unanimous Senate vote that struck a blow for the privacy rights of Americans.

>> <http://www.net-security.org/news.php?id=1945>

RESPONDING IN KIND

Microsoft Security Response Center revamps its advisory and patch processes.

>> <http://www.net-security.org/news.php?id=1949>

WEB SERVICES GROUP STILL SEEKING SECURITY

A group working to ensure the compatibility of Web services software is preparing to tackle its biggest challenge yet: Security.

>> <http://www.net-security.org/news.php?id=1950>

THE BIG LESSONS OF A LITTLE WORM

If Slammer's weekend assault had come just 48 hours later, the end result might have been a virtual Net shutdown. Institutional investors unable to make trades could have lost billions of dollars.

>> <http://www.net-security.org/news.php?id=1951>

SMALLPOT: TRACKING THE SLAPPER AND SCALPER UNIX WORMS

This article will look at the Smallpot Project, a generic honeypot designed to track almost any malware on the Internet, using the Slapper and Scalper worms as a case study.

>> <http://www.net-security.org/news.php?id=1952>

SECURE YOUR DNS - REPLACE BIND

BIND has become the most popular DNS server on the Internet. It is also a favorite attacker target. For organisations that require a more secure DNS infrastructure, the djbdns package may be the answer.

>> <http://www.net-security.org/news.php?id=1953>

THE CRYPTO GARDENING GUIDE AND PLANTING TIPS

The intent of this document is to cover some of the real-world constraints for cryptographers, to point out problems that their designs will run into when attempts are made to deploy them.

>> <http://www.net-security.org/news.php?id=1954>

ACTIVESTATE PUREMESSAGE TESTED FOR UNIXREVIEW

PureMessage is a full-featured mail filtering system that can be used as a combination filter/MTA solution or a standalone filter that passes messages on to a MTA for delivery. Here's a test.

>> <http://www.net-security.org/news.php?id=1955>

MAC TURNS SECURITY GUARD

A Mac video motion-detection package has been released as a home-and-office security solution.

>> <http://www.net-security.org/news.php?id=1958>

BUSH'S DATABASE FACES PRIVACY, NOT TECHNICAL, CONCERNS

Bush's plan for a massive antiterrorism database center, could be up and running within months from a technology standpoint, but harder to overcome will be privacy concerns of a non-technical nature.

>> <http://www.net-security.org/news.php?id=1959>

WORM SPREAD WORLDWIDE IN 10 MINUTES

It only took 10 minutes for the SQL Slammer worm to race across the globe and wreak havoc on the Internet two weeks ago, making it the fastest-spreading computer infection ever seen.

>> <http://www.net-security.org/news.php?id=1960>

OPEN WIRELESS NETWORKS POSE DILEMMA

If you want to know how unsecure today's wireless networks are, just ask the people who make it their mission to locate the access points designated by companies and consumers around the world.

>> <http://www.net-security.org/news.php?id=1961>

ONLINE CHILD PORN ARRESTS TOTAL 1,600

More than 1,600 men have so far been arrested in Operation Ore, the huge UK police investigation into child porn on the internet.

>> <http://www.net-security.org/news.php?id=1962>

THE GREAT IDS DEBATE

In this article, we'll examine and compare the two different techniques: signature analysis and protocol analysis.

>> <http://www.net-security.org/news.php?id=1963>

INDIA GETS ITS FIRST CYBER CONVICT

A 24-year-old engineer from Delhi has earned the dubious distinction of being the first person in India to be convicted for a cyber crime. A city court convicted Asif Azim for using an American citizen's credit card to make an online purchase.

>> <http://www.net-security.org/news.php?id=1964>

SECURE CONFIGURATION OF SERVERS STOPS SQLSLAMMER AND OTHERS

Here are some basic protection measures, with a particular emphasis on those that provide Internet services.

>> http://www.net-security.org/virus_news.php?id=181

WEB WORM SUSPECTS BAILED

Two people suspected of creating the TK web worm have been released on bail.

>> <http://www.net-security.org/news.php?id=1968>

ISA TO CONSUMERS: THINK SECURITY

A coalition of technology companies and others doing business on the Internet have released a list of nine steps they believe consumers should take to protect themselves.

>> <http://www.net-security.org/news.php?id=1969>

BROTHER, CAN YOU SPARE SOME PRIVACY?

Companies that wish to display the TRUSTe seal on their Web site will have to demonstrate a higher level of privacy protection.

>> <http://www.net-security.org/news.php?id=1970>

THE HACKERS ARE COMING TO TOWN

There was a time when the term hacker, even to the generalist, was nothing uncomplimentary. There were people of all ages who had this urge to fiddle with computer hardware or meddle with code.

>> <http://www.net-security.org/news.php?id=1971>

MAN CHARGED WITH HACKING VIEWSONIC SYSTEM

A former employee of ViewSonic Corp. was arrested on Thursday for allegedly hacking into its computer system and destroying data, shutting down a server that was central to the firm's foreign operations.

>> <http://www.net-security.org/news.php?id=1972>

STALKERS USE GPS TO TRACK VICTIMS

Two recent cases in which stalkers used global positioning system receivers to follow their victims' movements spark concern among law enforcement. Meanwhile, police install GPS systems of their own.

>> <http://www.net-security.org/news.php?id=1973>

STUDENT CHARGED WITH HACKING AND INFORMATION THEFT

A Boston College student was indicted on charges he penetrated the campus computers, gathered personal information on more than 4,000 people, and stole about \$2,000 in goods and services.

>> <http://www.net-security.org/news.php?id=1974>

[Vulnerabilities]

All vulnerabilities are located here:

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

HPUX Wall Buffer Overflow Vulnerability

>> <http://www.net-security.org/vuln.php?id=2421>

AbsoluteTelnet 2.00 Buffer Overflow Vulnerability

>> <http://www.net-security.org/vuln.php?id=2420>

PHPMyNewsLetter Unauthorised File Access Vulnerability

>> <http://www.net-security.org/vuln.php?id=2419>

TOPo upto v.1.43 Path Disclosure Vulnerability

>> <http://www.net-security.org/vuln.php?id=2418>

WebSphere 4.0.4 XML Configuration Export Weak Password Protection

>> <http://www.net-security.org/vuln.php?id=2417>

Majordomo Information Leakage Vulnerability

>> <http://www.net-security.org/vuln.php?id=2416>

Snatching Visited Websites from Opera

>> <http://www.net-security.org/vuln.php?id=2415>

Opera "History" Privacy Breach

>> <http://www.net-security.org/vuln.php?id=2414>

Opera Images Cross Site Scripting Vulnerability

>> <http://www.net-security.org/vuln.php?id=2413>

Phantom of the Opera - Attacker Can Gain Access to file:// Protocol

Opera's Security Model is Highly Vulnerable
>> <http://www.net-security.org/vuln.php?id=2411>

PHP-Nuke Avatar Code Injection Vulnerability
>> <http://www.net-security.org/vuln.php?id=2410>

Kazaa Media Desktop v2 Denial of Service Vulnerability
>> <http://www.net-security.org/vuln.php?id=2409>

phpMyShop SQL Injection Vulnerability
>> <http://www.net-security.org/vuln.php?id=2408>

myphpPagetool Include File Vulnerability
>> <http://www.net-security.org/vuln.php?id=2407>

3Ware 3DM Denial of Service Vulnerability
>> <http://www.net-security.org/vuln.php?id=2406>

Compaq Web Agent Management Session Can be Re-Used
Without The Need To Perform Authentication
>> <http://www.net-security.org/vuln.php?id=2405>

HNS Book Giveaway: <http://net-security.org/news.php?id=1980>
> Firewalls and Internet Security: Repelling the Wily Hacker 2/e
> Managing Information Security Risks: The OCTAVE Approach

[Advisories]

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

Red Hat Security Advisory - Updated kernel-utils packages
fix setuid vulnerability
>> <http://www.net-security.org/advisory.php?id=1581>

Red Hat Security Advisory - Updated w3m packages fix
cross-site scripting issues
>> <http://www.net-security.org/advisory.php?id=1580>

Red Hat Security Advisory - Updated Xpdf packages fix
security vulnerability
>> <http://www.net-security.org/advisory.php?id=1579>

Red Hat Security Advisory - Updated WindowMaker packages fix vulnerability in theme-loading
>> <http://www.net-security.org/advisory.php?id=1578>

Red Hat Security Advisory - Updated openldap packages available
>> <http://www.net-security.org/advisory.php?id=1577>

Microsoft Security Bulletin MS03-004 - Cumulative Patch for Internet Explorer
>> <http://www.net-security.org/advisory.php?id=1576>

Microsoft Security Bulletin MS03-005 - Unchecked Buffer in Windows Redirector Could Allow Privilege Elevation
>> <http://www.net-security.org/advisory.php?id=1575>

Mandrake Linux Security Advisory - slocate
>> <http://www.net-security.org/advisory.php?id=1574>

Mandrake Linux Security Advisory - kernel
>> <http://www.net-security.org/advisory.php?id=1573>

Conectiva Linux Security Announcement - mrcrypt
>> <http://www.net-security.org/advisory.php?id=1572>

Gentoo Linux Security Announcement - bladeenc
>> <http://www.net-security.org/advisory.php?id=1571>

FreeBSD Security Advisory - remotely exploitable vulnerability in cvs server
>> <http://www.net-security.org/advisory.php?id=1570>

Gentoo Linux Security Announcement - qt-dcgui
>> <http://www.net-security.org/advisory.php?id=1569>

Red Hat Security Advisory - Updated PHP packages available
>> <http://www.net-security.org/advisory.php?id=1568>

Red Hat Security Advisory - Updated 2.4 kernel fixes various vulnerabilities
>> <http://www.net-security.org/advisory.php?id=1567>

Mandrake Linux Security Advisory - mysql
>> <http://www.net-security.org/advisory.php?id=1566>

Mandrake Linux Security Advisory - vim
>> <http://www.net-security.org/advisory.php?id=1565>

Red Hat Security Advisory - Updated kerberos packages
fix vulnerability in ftp
>> <http://www.net-security.org/advisory.php?id=1564>

Gentoo Linux Security Announcement - slocate
>> <http://www.net-security.org/advisory.php?id=1563>

Gentoo Linux Security Announcement - Mail-SpamAssasin
>> <http://www.net-security.org/advisory.php?id=1562>

SCO Security Advisory - Linux: CVS double free vulnerability
>> <http://www.net-security.org/advisory.php?id=1561>

[**Featured articles**]

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

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

Interview with Dr. Nicko van Someren, CTO of nCipher
>> <http://www.net-security.org/article.php?id=380>

Interview with Ratmir Timashev, CEO of Aelita Software
>> <http://www.net-security.org/article.php?id=379>

The Advantages of Block-Based Protocol Analysis for Security Testing
>> <http://www.net-security.org/article.php?id=378>

Trend Micro Announces Q4 2002 Earnings
>> <http://www.net-security.org/article.php?id=377>

Webcast - Eliminate the SANS/FBI Top 20 Internet Vulnerabilities
>> <http://www.net-security.org/article.php?id=376>

Interview with Steven Dabbs, CEO & President of ScannerX
>> <http://www.net-security.org/article.php?id=375>

HNS Book Giveaway: <http://net-security.org/news.php?id=1980>
> Firewalls and Internet Security: Repelling the Wily Hacker 2/e
> Managing Information Security Risks: The OCTAVE Approach

[**Reviews**]

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

MANAGING INFORMATION SECURITY RISKS: THE OCTAVE APPROACH

This book provides a powerful documentation on CERT/CC's Operationally Critical Threat, Asset, and Vulnerability Evaluation. It offers all the information you need to know while thinking about or starting the implementation of the OCTAVE into your organization.

>> <http://www.net-security.org/review.php?id=29>

COUNTER HACK: A STEP-BY-STEP GUIDE TO COMPUTER ATTACKS AND EFFECTIVE DEFENSES

If you're in charge of the security of a network or just a security enthusiast, you'll find this book of great value. The specific tools and techniques described in this book are more valuable than just theory presented in other publications.

>> <http://www.net-security.org/review.php?id=30>

[**Security world**]

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

ActivCard Announces Final Results of Exchange Offer for Reincorporation

>> <http://www.net-security.org/press.php?id=1239>

TruSecure and IP3 Inc. Announce Education Partnership

>> <http://www.net-security.org/press.php?id=1238>

Zix Corporation Introduces ZixWorks, a Fully Managed and Hosted Email Protection Service

>> <http://www.net-security.org/press.php?id=1237>

Trend Micro Delivers Enterprise-level Outbreak Prevention and
Damage Cleanup Services for Networked Computers and Servers
>> <http://www.net-security.org/press.php?id=1236>

iLottery System Goes Mobile
>> <http://www.net-security.org/press.php?id=1235>

iPass Improves its Enterprise Connectivity Offerings
For PDA Devices and Mac OS X
>> <http://www.net-security.org/press.php?id=1234>

Datakey Introduces Model 330J Java Card
>> <http://www.net-security.org/press.php?id=1233>

Equipped with Arbor Networks' Peakflow, Rackspace
Managed Hosting Staves Off SQL Worm
>> <http://www.net-security.org/press.php?id=1232>

[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

PRODETECT 0.1B

proDETECT is an open source promiscuous mode scanner with a
GUI. It uses ARP packet analyzing technique to detect adapters
in promiscuous mode.

>> <http://www.net-security.org/software.php?id=445>

MALLOC() SLOWSCAN 0.0.1B

Malloc() SlowScan is a tool used to perform TCP port scanning in
a a unique way. To avoid detection from IDS's like: Snort , ISS
BlackICE defender, The CrunchBox and possibly others.

>> <http://www.net-security.org/software.php?id=446>

FWTRENDS 0.1.1

fw trends is a project to ease firewall log monitoring via a Web
GUI. It imports log files from various firewall software and can
easily generate graph statistics from alert events.

>> <http://www.net-security.org/software.php?id=447>

TINY SHELL 0.31

This is a lightweight client/server clone of the standard remote shell tools (rlogin, telnet, ssh, etc.), which provides remote shell execution and file transfers.

>> <http://www.net-security.org/software.php?id=448>

[Virus News]

All virus news are located at:

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

Helkern / SQL Worm - The Fastest Ever

>> http://www.net-security.org/virus_news.php?id=183

Sophos Reports Record Momentum in 2002

>> http://www.net-security.org/virus_news.php?id=182

Secure Configuration of Servers Stops SQLSlammer and Others

>> http://www.net-security.org/virus_news.php?id=181

BBC's The Archers Sends Out Virus

>> http://www.net-security.org/virus_news.php?id=180

Kaspersky Labs: Virus Top 20 for January 2003

>> http://www.net-security.org/virus_news.php?id=179

Klez.I heads Panda ActiveScan's Top Ten

>> http://www.net-security.org/virus_news.php?id=178

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

*** **ALERT!** ***

ALL OF THE FOLLOWING APPLICATIONS ARE VULNERABLE TO ATTACK!:

- *** Microsoft SQL Server
- *** Lotus Domino
- *** IBM DB2/UDB
- *** Oracle
- *** Sybase

Get a **FREE SAMPLE VULNERABILITY ASSESSMENT** of your DATABASE and APPLICATIONS from:

<http://www.appsecinc.com/helpnetsecurity/>

QUESTIONS: How Vulnerable are Your Applications and Databases? Are Your Databases Secured to Resist Another SQL Slammer/Sapphire Worm? Are You Confident Enough to Say That Your Applications and Databases Are Secure from Future Attacks?

ANSWER: Find out now and get a **FREE SAMPLE VULNERABILITY ASSESSMENT** of your DATABASE and APPLICATIONS from:

<http://www.appsecinc.com/helpnetsecurity/>
