

HNS Newsletter  
Issue 74 - 05.08.2001  
<http://net-security.org>  
<http://security-db.com>

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://www.net-security.org>.

Subscribe to this weekly digest on:  
<http://www.net-security.org/text/newsletter>

Archive of the newsletter in TXT and PDF format is available here:  
<http://www.net-security.org/news/archive/newsletter>

Table of contents:

- 1) General security news
- 2) Security issues
- 3) Security world
- 4) Featured products
- 5) Featured article
- 6) Security software
- 7) Defaced archives

=====  
HAL 2001

=====  
Between 10th and 12th August, thousands of hackers will populate the green fields of the campus of the University of Twente, converting it into a large doubleplus-extrawired campsite. When not visiting lectures or workshops, we'll be engaged in technical or political discussions, or maybe just relaxing somewhere in the grass.

If you can truly celebrate the Internet and embrace new technologies, without forgetting your responsibility to tell others that new technologies come with new risks to the individual and to society as a whole, then this is the place to be this summer. To be sure of an entrance ticket, register now! Visit us at <http://www.hal2001.org>  
=====

General security news  
-----

=====  
CODE RED SPECIAL COVERAGE

=====  
In order to make things easier to find, all the information regarding the worm are in this page. Everything from alerts, news items, solutions, etc.

<http://www.net-security.org/text/articles/coverage/code-red>  
=====

### THE FIREWALL FETISH

If security is the problem, a firewall is only part of the solution. Firewalls are the bestsellers of tech security, cheap, formulaic and popular. Like a good paperback, they offer a pleasant escape from reality.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cio.com/forums/security/edit/a072601\\_firewall.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cio.com/forums/security/edit/a072601_firewall.html)

### HACK ATTACK TARGETS VERIZON, AT&T WIRELESS USERS

Verizon wireless and AT&T Wireless Group have started investigations into a security breach that may have allowed outsiders to see confidential information of at least hundreds of their customers. Officials from Verizon and AT&T confirmed that they are looking into an apparent security breach that permitted information of a number of users to be circulated publicly in Internet chat rooms.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://iwsun4.infoworld.com/articles/hn/xml/01/07/30/010730hnverup.xml>

### CSEAT WILL REVIEW AGENCIES' SECURITY FOR FREE

The National Institute of Standards and Technology has set up a computer security expert assist team, called CSEAT, to improve agencies' infrastructure protection and share best security practices. "It was kind of a surprise" to get a budget line item for CSEAT, said its director, Kathy Lyons-Burke. "We didn't expect Congress to give us the money."

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.gcn.com/vol1\\_no1/daily-updates/4768-1.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.gcn.com/vol1_no1/daily-updates/4768-1.html)

### SOME HEAVY RANTING

Rob Rosenberger - "Today's antivirus technology died nine years ago according to Steve Gibson. Why didn't his ancient prophesy of doom come true?". The Register's Thomas C. Greene wrote a new article - "Code Red Tribulation is nigh, Steve Gibson warns".

Link: <http://vmyths.com/rant.cfm?id=348&page=4>

### SIRCAM LATEST STATISTICS

MessageLabs - "We have also seen a number of doubly infected files, such as SirCam infected with FunLove, or SirCam infected with Kriz. There is a potential problem here with virus scanners that disinfect files. It is theoretically possible for a scanner to imperfectly disinfect this kind of file, perhaps removing FunLove."

Link: <http://www.messagelabs.co.uk/viruseye/report.asp?id=72>

### THE FOUNDER OF THE CHAOS COMPUTER CLUB DIED

The CCC now has to continue without its honorary president Wau Holland, also known as Herwart Holland-Moritz. Holland suffered a stroke in late May and fell into a coma; he died Sunday morning, age 49. Read today, Holland's editorial that appeared in the first issue of CCC's magazine "Datenschleuder" (roughly: "data sling") back in 1984 appears almost visionary. For him and for the CCC, the computer was already not merely a technology but "the most important new medium." He held that "all existing media will be increasingly networked through computers, a networking which creates a new quality of media."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.thestandard.com/article/0,1902,28349,00.html>

## VIRUSES OF THE 21ST CENTURY

The definition of a virus would be a piece of computer code that propagates itself, and spreads to as many different hosts as possible. In the real world this can be seen through epidemics like the Flu. In computer land, there are no 6 degree's of separation. Everyone is accessible by just one step, one email address, one common and easily accessible route to penetration and being infected by a virus.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theinquirer.net/31070106.htm>

## LAPTOP SECURITY, PART ONE: PREVENTING LAPTOP THEFT

This article, the first in a two-part series devoted to laptop security, will give a brief overview of how users can prevent laptop theft. In realization of the fact that no matter what users do, laptop theft will always be a possibility, the second article in this series will discuss steps that users can take to minimize the loss of valuable information through laptop theft.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/basics/articles/laptop1.html>

## LEGAL BATTLE BREWING OVER RELEASE OF TELNET EXPLOIT?

While acknowledging that he had been in error in publishing the exploit, Levy said, "We do not encourage people that find vulnerabilities to release exploits, although we understand that some people may think it's necessary. We encourage people that wish to release some type of demonstration tool to create it in such a way that it only allows for the testing, not the exploitation, of the vulnerability. That being said, if there is an exploit in the wild we will publish it so as to allow the public to be aware of its existence, study it, and use it for their own testing."

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.internetnews.com/wd-news/article/0,,10\\_855121,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.internetnews.com/wd-news/article/0,,10_855121,00.html)

## SUB7 COMES BACK

First touted at the Def Con conference earlier this month, the tool has finally been released in Alpha form. Sub7 has been ported over to the Mac from the original Windows code by group Team2600, which claims to be the world's oldest Macintosh user group. This means that Mac OS users are now susceptible to the tool which allows a user to remotely take complete.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1124342>

## SECURITY FEARS ARE BARRIER FOR P2P NETWORKING TAKE-OFF

Peer to peer networking is entering the corporate mainstream but users will need convincing that security concerns can be addressed. That's one of the main conclusions of a study by industry analysts Frost & Sullivan, US Enterprise Peer-to-Peer Networking Markets, which estimated that 61,400 enterprise users have access to peer-to-peer (P2P) networks and this figure will rise to 6.2 million by 2007.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/5/20733.html>

## ECHELON UPDATE

"We've gone past the point where Echelon is 'X-Files' material and can be

dismissed as paranoia," said Barry Steinhardt, associate director of the New York office of the American Civil Liberties Union, which maintains the Echelon Watch Web site.

Link: <http://www.sfgate.com/cgi-bin/article.cgi?f=/chronicle/archive/2001/07/30/BU225644.DTL>

#### NOKIA INTRODUCES NEW FIREWALL/VPN APPLIANCE

Nokia Corp. has introduced the smallest of its firewall/VPN appliances with management features designed for enterprise branch offices - IP71. It is based on Check Point Small Office software, a slimmed-down version of Check Point's VPN-1/Firewall-1 specifically made for low-cost, small office appliances with a limited number of users.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.itworld.com/Net/2880/NWW010731nokia/>

#### LYCOS OPEN TO MALICIOUS ATTACKS

The vulnerability allows malicious attacker to redirect unsuspected users to a bogus site or even run a malicious code in the user's machine. The risk is only a theoretical but could lead to a serious attack. Once the engine has completed a search the results page displays a short summary of each page. This description is gleaned from meta-tags attached to the web page. The tags, often in HTML or JavaScript, allow another script to be embedded within the text fields so the text can be a program that is automatically executed when the search engine displays the page summary.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.silicon.com/a46168>

#### HOW FAR CAN FBI SPYING GO?

Nicodemo S. Scarfo is an alleged mastermind of a loan shark operation in New Jersey. He's also the defendant in a case that could - depending on how a federal judge rules in the next few weeks - dramatically expand the government's powers to spy on Americans or restrict police to traditional techniques. To hear federal prosecutors tell it, the FBI became so frustrated by Scarfo's use of PGP to encode confidential business data that they had to resort to extraordinary means. With a judge's approval, FBI agents repeatedly snuck into Scarfo's business to plant a keystroke sniffer and monitor its output.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,45730,00.html>

#### PROTESTORS TURN ATTENTION TO DOJ

2600 reports that another round of worldwide protests occurred Monday in the case of arrested Russian programmer Dmitry Sklyarov.

Link: <http://www.2600.com/news/display.shtml?id=618>

#### SECURING AN UNPATCHABLE WEBSERVER... HOGWASH!

Hogwash is a Snort-based packet scrubber designed to take out 95% of the stock attacks hackers may throw at a network. Hogwash lives inline like a firewall, but it works differently. Instead of closing ports like a traditional firewall, it drops or modifies specific packets based on a signature match. This article by the developers of Hogwash will give a brief overview of the product.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/ids/articles/hogwash.html>

#### BRIAN MARTIN SPEAKS ABOUT ATTRITION DEFACEMENT

Thanks to Giordani Rodrigues for sending us a link to his interview with Brian Martin from Attrition. Jericho - "The remote compromise appears to be from Fluffy Bunny compromising a foreign system, backdooring it, sniffing an SSH session to this machine."

Link: [http://www.infoguerra.com.br/infonews/viewnews.cgi?newsid996659484,46499,](http://www.infoguerra.com.br/infonews/viewnews.cgi?newsid996659484,46499)

#### CYBER CASINO PLAN COULD BE SPIKED OVER SECURITY

Plans for online gaming in Nevada could be put on ice because industry regulators say they cannot guarantee security. Internet gaming consultant James Sargent said web casinos are constantly at risk for money laundering, identity and credit card theft.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.ananova.com/news/story/sm\\_364765.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.ananova.com/news/story/sm_364765.html)

#### MAC OS X FIREWALL CONFIG UTILITY

Firewalk is a Mac OS X configuration utility for the built in firewall. While you are running Mac OS X you should be aware that you are running on a BSD/Mach kernel. The built in firewall that Mac OS X offers is rather dirty, some like to get into the unix part of the operating system others still prefer the nice Macintosh GUI.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securemac.com/macosexfirewalk.php>

#### SENATOR TARGETS SCHOOL HACKERS

Sen. Robert Torricelli claims he wants to put hackers who disrupt school computers in prison. But educators, programmers and civil libertarians say Torricelli's recently-introduced School Website Protection Act of 2001 does more than place wrongdoers behind bars. They say the bill is worded so vaguely it would turn commonplace activities into federal crimes to be investigated by the U.S. Secret Service.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,45752,00.html>

#### AN AUDIT OF ACTIVE DIRECTORY SECURITY, PART ONE

This article is the first in a series that will discuss some potentially major security issues that may exist in the implementation of Active Directory. As Active Directory is a very large, complicated technology, these articles will come nowhere near reviewing the entirety of the subject. This installment will offer a brief overview of Active Directory, as well as a very introductory look at some of the security issues surrounding it.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/microsoft/2k/adaudit1.html>

#### IMPLEMENTING SECURITY IN FREEBSD UNIX SYSTEM

The funny thing about security is that we actually have quite a lot of it in the UNIX paradigm. We have users, groups, chroot, secure levels, and jails. The only problem is that we don't use any of it by default. Most services are run as root - pop3, ftp, ssh, ident, sendmail, talkd, named, ntpd, and even the ones that aren't, such as apache, barely touch the first layer of security offered in FreeBSD: each runs as its own user and group but doesn't bother with anything else.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.daemonnews.org/200108/security\\_overview.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.daemonnews.org/200108/security_overview.html)

#### 8 KEYS TO A SANE SECURITY STRATEGY

Well, it's finally happened: security and its first cousin, privacy, are now household requirements. Ignore them and you're toast. How did this happen so fast? Blame it on distributed computing and the distributed steroid known as the Internet. As business models moved into cyberspace, we found ourselves facing new threats. We're now surrounded by security and privacy technologies, officers, consultants, and regulators.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://itmanagement.earthweb.com/secu/article/0,,11953\\_855161,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://itmanagement.earthweb.com/secu/article/0,,11953_855161,00.html)

#### SECURE TEXT MESSAGING TECHNOLOGY PREVENTS FORWARDING

A new secure method for sending tickets electronically to mobile phones has been unveiled from start-up firm Link77. Known as Ticket Mobile, the system allows for non-standard (non-ASCII) characters to be included in the message header of a text message, a technique that generates a security symbol alongside the message on the recipient's mobile phone.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/168585.html>

#### FTC EYEING NEW IT SECURITY RULES

The U.S. Federal Trade Commission (FTC) is considering a new set of security rules that could affect the information security practices at a swath of businesses. And although the FTC says the hallmark of the rules will be flexibility, industry analysts say it will still give IT managers something to worry about.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/storyba/0,4125,NAV47\\_STO62715,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/storyba/0,4125,NAV47_STO62715,00.html)

#### INTERNET SECURITY

The focus of Internet security is to ensure private, authenticated communications between parties over the Internet, Extranets, or Intranets. This article provides an overview of Internet security, which involves many technologies to authenticate users, restrict access, and encrypt data.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www-1.ibm.com/servers/eserver/series/beyondtech/internet\\_security.htm](http://www.net-security.org/cgi-bin/news.cgi?url=http://www-1.ibm.com/servers/eserver/series/beyondtech/internet_security.htm)

#### NETWORK SECURITY POLICY

Without a security policy, the availability of your network can be compromised. The policy begins with assessing the risk to the network and building a team to respond. Continuation of the policy requires implementing a security change management practice and monitoring the network for security violations. Lastly, the review process modifies the existing policy and adapts to lessons learned.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cisco.com/warp/public/126/secpol.html>

#### WHAT YOU CAN DO IF YOUR SECURITY VENDOR FAILS

Pilot Network Services customers had to scramble when the managed security company suddenly went under. They soon learned that outsourcing security is

a lot more complicated than they thought.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cio.com/archive/080101/exposed.html>

#### ALERTS IN THE RIGHT TIME?

Ronald Dick, head of the FBI's National Infrastructure Protection Center (NIPC) said that had not public outreach taken place, including the alerting of the nation's ISPs, at least 350,000 servers could have been compromised by today.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/168610.html>

#### SIRCAM AND HIS FAMOUS VICTIMS

The SirCam worm has claimed a new victim, the confidential President of the Ukraine Leonid Kuchma. It looks like staff of Ukrainian news website ForUm got an infected mail with one of the documents that would be a secret.

Link:

<http://www.silicon.com/public/door?REQUNIQ=996770059&6004REQEVENT=&REQINT1=46240>

#### BUILDING AND DEPLOYING OPENSSSH FOR SOLARIS

This article describes how to build and deploy OpenSSH for the Solaris Operating Environment (Solaris OE) to enable secure remote network connections with strong authentication and encryption.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sun.com/blueprints/0701/openSSH.html>

#### AN ANALYSIS OF THE VBSWG WORM KIT

The Homepage and the Anna Kournikova worms are two high-profile examples of the VBS/VBSWG@mm family of visual basic script worms. These worms are generated by the VBSWG kit, one of the many virus-generating kits that are easily available on the Internet. These kits make writing a virus a simple, straightforward and unskilled task. Given the prominence of this kit, and its related worms, it would be useful for security and virus professionals to better understand it.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/virus/articles/viruskit.html>

#### STEALTH FIGHTERS - ANTIVIRUS PROGRAMS

To trap viruses that the antivirus companies have not yet analyzed, antivirus utilities use a method called heuristics; that is, the programs scan not for a particular signature, but for certain types of behavior. This technique can lead to problems, however, when the utility mistakes an innocent file for a virus. Other antivirus programs are common sources of false positives, too: If you install one such program on top of another, the new program may assume that the virus signatures of the original program are viruses.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.pcworld.com/reviews/article/0,aid,55803,00.asp>

#### CIPHER ATTACK DELIVERS HEAVY BLOW TO WLAN SECURITY

A new report dashes any remaining illusions that 802.11-based (Wi-Fi) wireless local-area networks are in any way secure. The paper, written by three of the

world's foremost cryptographers, describes a devastating attack on the RC4 cipher, on which the WLAN wired-equivalent privacy (WEP) encryption scheme is based.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.eetimes.com/story/OEG20010803S0082>

#### WHAT EXACTLY IS PKI? AND WHO NEEDS IT?

PKI is a catchall term for the infrastructure required to manage digital certificates and highly secure encryption. It encompasses a great deal: industry standards, software and hardware systems, business processes and security policies – even human resources within a company responsible for carrying out various "trust processes."

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www-3.ibm.com/security/library/wp\\_pki1.shtml](http://www.net-security.org/cgi-bin/news.cgi?url=http://www-3.ibm.com/security/library/wp_pki1.shtml)

#### SIRCAM'S WORM COCKTAILS PACK A WALLUP

As the Code Red worm this week reprised its role as Internet uber-threat and media darling, the far more malicious and far less famous SirCam worm continued to infect thousands of PCs a day, e-mailing sensitive documents from those systems at random.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/eweek/stories/general/0,11011,2801786,00.html>

#### COMMERCE COMPUTER SECURITY LACKING

The Commerce Department's computer networks, which contain some of America's most valuable business secrets, have security holes easily accessible to Internet criminals, federal investigators say.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computeruser.com/news/01/08/05/news1.html>

#### YOUR NETWORK'S SECRET LIFE, PART 4

xinetd features a number of enhancements over good old inetd, including extensive logging capabilities, limits on incoming connections (to prevent denial of service attacks), flexible access control for both local and remote connections, and much more (as they say on TV).

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www2.linuxjournal.com/articles/sysadmin/0062.html>

#### MUELLER NONCOMMITTAL ON CARNIVORE

FBI Director Robert Mueller has refused to commit to an independent review of the agency's Carnivore surveillance system. During an appearance before the Senate Judiciary committee on Tuesday, Mueller said he couldn't promise another look at the controversial technology, which the FBI has renamed DCS1000. The Senate later confirmed Mueller in a 98-0 vote.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://wired.com/news/politics/0,1283,45798,00.html>

-----

## Security issues

---

All vulnerabilities are located at:  
<http://net-security.org/text/bugs>

---

### KAZAA + MORPHEUS SHARING FILES

I've found a bug in Kazaa 1.3.1 and Morpheus 1.3. I'll refer to them as K/M. I've found this bug to occur when the download directory is changed from the default "My Shared Folder" to something else. In K/M go to Tools menu and choose Options. Under the Downloads and uploads tab change the folder for downloaded files to something else, for example c:\downloads. Now choose Find media to share... from the Tools menu and click on Folder List. Click Deselect all to make sure you aren't explicitly sharing any files. Close K/M and remove it from the tray. Now open K/M again. Connect to <http://yourip:1214> in your web browser and you should see some files. If you don't, try changing your downloaded folders location to something like c:\ or c:\windows.

Link: <http://www.net-security.org/text/bugs/996496175,41008,.shtml>

### DEBIAN SECURITY ADVISORY: APACHE REMOTE EXPLOIT

A problem in the package could allow directory indexing, and path discovery. In a default configuration, Apache enables `mod_dir`, `mod_autoindex`, and `mod_negotiation`. However, by placing a custom crafted request to the Apache server consisting of a long path name created artificially by using numerous slashes, this can cause these modules to misbehave, making it possible to escape the error page, and gain a listing of the directory contents.

Link: <http://www.net-security.org/text/bugs/996496343,41879,.shtml>

### TREND MICRO APPLLETTRAP SCRIPT FILTERING PROBLEMS

AppletTrap includes some design and implementation flaws, which allow an attacker to bypass restrictions set by the product administrator and introduce malicious code into an organization.

Link: <http://www.net-security.org/text/bugs/996496442,33719,.shtml>

### MICROSOFT DCE/RPC DEAMONS DoS

An unauthenticated remote attacker that can talk to the endpoint on which the server is listening can crash the server. In some cases, the servers may either restart themselves, or be restarted by the OS.

Link: <http://www.net-security.org/text/bugs/996577527,52822,.shtml>

### MATHEMATICA LICENSE MANAGER VULNERABILITIES

Two not too serious bugs in the network license manager (`mathlm`) for Mathematica versions 4.0 and 4.1, on at least the Intel linux platform, probably every version and every platform. These can both lead to a denial of service on `mathlm` (stopping legitimate machines from getting licenses to run the mathematica kernel), and the latter can lead to the granting of a mathematica license for a machine which shouldn't be granted a license.

Link: <http://www.net-security.org/text/bugs/996577657,3189,.shtml>

#### QUAKE 3 ARENA 1.29F/G VULNERABILITY

There exists a very large hole in Quake 3 Arena, version 1.29f and 1.29g (the latest, 1.29g which got released just under a week ago). The hole is not fixable in any way by the user, and most of the servers that are up (thousands of them) are vulnerable. To have this hole fixed, a PR (point release) will have to be given to the public by iD Software.

Link: <http://www.net-security.org/text/bugs/996577740,1826,.shtml>

#### COMMAND EXECUTION VULNERABILITY IN MYPHPADMIN

The new method involves an unchecked variable in the 'tbl\_copy.php' and 'tbl\_rename.php' scripts. By passing a carefully crafted URL to these scripts, it is possible to insert PHP instructions into an eval() function thereby enabling the attacker to execute arbitrary commands on the webserver with the privileges of the http daemon, typically 'nobody'.

Link: <http://www.net-security.org/text/bugs/996598920,40154,.shtml>

#### KRB5 TELNETD BUFFER OVERFLOWS

Buffer overflows exist in the telnet daemon included with MIT krb5. Exploits are believed to exist for various operating systems on at least the i386 architecture.

Link: <http://www.net-security.org/text/bugs/996661316,99267,.shtml>

#### IBM AIX - BUFFER OVERFLOW IN TELNET DAEMON

In the AIX version of "telnetd", as well as most other versions of "telnetd" derived from the BSD telnet daemon, there exists a buffer overflow vulnerability in telrcv(), the function that processes various options under telnet. There is an output buffer in the function that holds the information gathered during the parsing of the option request and the daemon's internal state. This buffer is not bounds checked, allowing for the possibility of forcing an overflow condition in the stack when the buffer returns its data to the telnet client.

Link: <http://www.net-security.org/text/bugs/996661549,7633,.shtml>

#### FREEBSD SECURITY ADVISORY - TELNETD VULNERABILITY

An overflowable buffer was found in the version of telnetd included with FreeBSD. Due to incorrect bounds checking of data buffered for output to the remote client, an attacker can cause the telnetd process to overflow the buffer and crash, or execute arbitrary code as the user running telnetd, usually root. A valid user account and password is not required to exploit this vulnerability, only the ability to connect to a telnetd server.

Link: <http://www.net-security.org/text/bugs/996682890,8634,.shtml>

#### VULNERABILITIES IN CISCO SN 5420 STORAGE ROUTERS

Two vulnerabilities have been discovered in Cisco SN 5420 Storage Router software release up to and including 1.1(3). One of the vulnerabilities can cause Denial-of-Service attack. The other allows unrestricted low level access to the SN 5420.

Link: <http://www.net-security.org/text/bugs/996710645,20609,.shtml>

#### ORACLE 8.1.5 DBNSMP VULNERABILITY

There is a problem in dbnsmpp that can be used by local users to obtain root

privileges. The dbnmp is setuid root. When a user execute dbnmp there is a call to chown and chgrp, but without specify the path, so any user can define his PATH variable to exploit this vulnerability.

Link: <http://www.net-security.org/text/bugs/996710696,36841,.shtml>

#### SLACKWARE 8.0, 7.1 VULNERABILITY: /USR/BIN/LOCATE

In slackware, and possibly other distributions, it is possible to modify the locate database if one were to obtain UID nobody. This allows locate to act as a sort of 'trojan' having anyone who executes it unknowingly execute potentially malicious code.

Link: <http://www.net-security.org/text/bugs/996710769,21304,.shtml>

#### MS01-035 HOT FIX FOR IIS

Basically, installing MS01-035 causes the IIS MMC to close when you click on the server extensions tab under Windows 2000 Advanced Server on SP2 (with all current hotfixes). Uninstalling MS01-035 fixes the problem, but opens up the security hole. This, I claim, is a broken solution.

Link: <http://www.net-security.org/text/bugs/996710889,94515,.shtml>

#### HP JETDIRECT PASSWORDS DON'T SYNC

If you configure the device through the web interface, and set the admin password, it does not create a password for the telnet interface.

Link: <http://www.net-security.org/text/bugs/996715376,64985,.shtml>

#### CALDERA LINUX - SECURITY PROBLEMS IN IMP

There are several security problems with IMP, a PHP based webmail application, shipped as part of OpenLinux 3.1 Server. These vulnerabilities allowed attackers to execute commands with the privileges of the httpd account.

Link: <http://www.net-security.org/text/bugs/996715469,43853,.shtml>

#### SUSE - SDBSEARCH.CGI VULNERABILITY

I found weakness in sdbsearch.cgi script which is a part of Suse distribution. This is perl script and since Suse 7.1 they have introduced some form of protection (interpreter is called with tainting checking). However, I think it isn't enough and this bug still may produce danger.

Link: <http://www.net-security.org/text/bugs/996834145,31937,.shtml>

#### SNMPD LOG FILES LONG NAMES PROBLEMS

when i launch snmpd with the arg's " -l AAAAAAAA...[455 char's]" i have a core dump... it's look like a little problem in the code when take the -l argument and strcpy to logfile, small buffer = core dump.

Link: <http://www.net-security.org/text/bugs/996834227,73054,.shtml>

#### TREND MICRO INTERSCAN VIRUSWALL VULNERABILITY

There is certain possibility of bypassing ISVW AV control. Affected version: 3.51 build 1321 for Windows NT (both CVP and Standard Ed.) TM released the patch, but it is not directly listed at patches download page.

Link: <http://www.net-security.org/text/bugs/996834281,59060,.shtml>

#### ROXEN WEBSERVER VULNERABILITY

Roxen Webserver 2.0 up to version 2.0.92 and 2.1 up to version 2.1.264 has a vulnerability that allows any user to retrieve any file from the host with the privileges of the web server. Having the CGI-module enabled escalates the problem by making it possible to run any executable.

Link: <http://www.net-security.org/text/bugs/996834377,35127,.shtml>

#### A DAMAGING LOCAL DOS IN WINNT SP6A

WindowsNT SP6a is subject to a local Denial of Service (DoS) attack, upon running "NT4ALL". This particular vulnerability has the potential to permanently damage the workstation/server, because no users are able to "log on" to the computer after NT4ALL is run.

Link: <http://www.net-security.org/text/bugs/996939945,40343,.shtml>

#### MULTIPLE VULNERABILITIES IN PHPNUKE

This is only possible if the intruder knows the database name that phpnuke is using, and the webserver must be able to connect to it without a password. Although It is very unlikely that these two circumstances will occur, but this is a bug still worth mentioning.

Link: <http://www.net-security.org/text/bugs/996940166,15531,.shtml>

#### PHPBB 1.4.0 VULNERABILITY

The problem lies in the fact that phpBB 1.4.x includes an algorithm in the auth.php file which removes backslashes that php automatically adds to GPC (Get/Post/Cookie) variables.

Link: <http://www.net-security.org/text/bugs/996940268,18669,.shtml>

-----  
  
Security world  
-----

All press releases are located at:  
<http://net-security.org/text/press>

-----  
  

#### INFOEXPRESS LAUNCHES CYBERARMOR 2.0 - [30.07.2001]

In response to the growing need for remote access security solutions that provide custom policy and enforcement tools, security pioneer InfoExpress is proud to announce the latest edition of its award-winning enterprise personal firewall suite: CyberArmor 2.0.

Press release:

< <http://www.net-security.org/text/press/996505018,40116,.shtml> >  
-----

SIDEWINDER FIREWALL IS NOT VULNERABLE - [31.07.2001]

Secure Computing Corporation, a leading provider of enterprise access control solutions, announced that its Sidewinder firewall and VPN gateway is not susceptible to the serious vulnerability that was reported in the recent CERT Advisory, CERT-2001-21. The Advisory reported that systems running versions of telnetd derived from BSD source code are vulnerable to an attack allowing unauthorized, complete, system access.

Press release:

< <http://www.net-security.org/text/press/996604683,71462,.shtml> >

-----

RSA SECURITY WILL ACQUIRE SECURANT TECHNOLOGIES - [31.07.2001]

RSA Security Inc. announced it has signed an agreement to acquire Securant Technologies, Inc., a privately held company that develops and delivers the award-winning ClearTrust authorization solution. The consideration for the acquisition is \$136.5 million in cash, plus acquisition costs. RSA Security will account for this transaction using purchase accounting. It is anticipated that the closing will occur in August 2001, subject to customary closing conditions, including obtaining required governmental approvals.

Press release:

< <http://www.net-security.org/text/press/996595763,24857,.shtml> >

-----

HUSH COMMUNICATIONS PREPARED FOR DIGITAL SIGS - [01.08.2001]

New legislation passed by the European Union now makes digital signatures officially legal in the EU, giving them equal status with hand-written signatures. Hush Communications, a leading provider of managed security services and key serving encryption technology, foreseeing such a development, already offers digital signatures as a standard feature of its secure communications solutions and, indeed, has just marked the successful launch of HushMail version 2.

Press release:

< <http://www.net-security.org/text/press/996661976,366,.shtml> >

-----

SYBARI'S SUPERIOR PROTECTION FROM SIRCAM - [03.08.2001]

Sybari Software, Inc., the premier developer of Antigen, a comprehensive antivirus, content-management, and e-mail security solution for Microsoft Exchange and Lotus Domino groupware servers, today reports that Antigen's Worm Purge and File Filtering have scored high-marks with Antigen users in the fight against one of the most destructive e-mail viruses since the "Love" virus.

Press release:

< <http://www.net-security.org/text/press/996836177,61773,.shtml> >

-----

SOPHOS: TOP TEN VIRUSES IN JULY 2001 - [04.08.2001]

This is the latest in a series of monthly charts counting down the ten most frequently occurring viruses as compiled by Sophos, a world leader in corporate anti-virus protection.

Press release:

< <http://www.net-security.org/text/press/996941018,29578,.shtml> >

-----

TREND MICRO POSTS RECORD FIRST-HALF REVENUE - [04.08.2001]

Trend Micro Incorporated, a leading provider of enterprise antivirus and content security software, today announced sales of 12,939 million yen for the first half of 2001, a 34.8% increase over the 9,600 million yen reported for the corresponding period of 2000, driven by rapid growth in North America and Europe.

Press release:

< <http://www.net-security.org/text/press/996941175,99470,.shtml> >

-----

Featured products

-----

The HNS Security Database is located at:  
<http://www.security-db.com>

Submissions for the database can be sent to: [staff@net-security.org](mailto:staff@net-security.org)

-----

LOGALERT

LogAlert is a web application audit and assessment tool, which automates web log analysis for IT and security professionals. This security software highlights and analyzes all suspicious behavior by categorizing the sequence of suspicious activities and providing detailed reporting on any intrusions that occur. Users can customize LogAlert reports for administrators who can then access them on a secure Web site for on-the-fly analysis. LogAlert handles all major Web servers, including Netscape, Microsoft IIS and Apache.

Read more:

< <http://www.security-db.com/product.php?id=809> >

This is a product of SPI Dynamics, for more information:

< <http://www.security-db.com/info.php?id=192> >

-----

## ON-LINE PORT SCAN

This scan in no way performs any operation that is destructive, nor does it attempt to capture private data of any kind except to relay back to you for your knowledge only. We simply scan for available ports and processes servicing those ports that appear to the public.

Read more:

< <http://www.security-db.com/product.php?id=733> >

This is a product of New Sky Internet Limited, for more information:

< <http://www.security-db.com/info.php?id=165> >

---

## REPORTING MODULE

Check Point's Reporting Module delivers actionable audit, trend and cost information from VPN-1 and FireWall-1 log file entries, presenting critical facts and relationships in simple, easy to understand reports. VPN-1 and FireWall-1 log file entries contain a rich set of information gathered while enforcing security policy rules. Each log file entry includes important network, security, and accounting data that can help security managers develop a detailed picture of network use and abuse. The Reporting Module's flexible consolidation, report definition, and report distribution capabilities transform this data into reports accessible to all levels of decision makers.

Read more:

< <http://www.security-db.com/product.php?id=425> >

This is a product of Check Point, for more information:

< <http://www.security-db.com/info.php?id=93> >

---

## Featured article

---

All articles are located at:  
<http://www.net-security.org/text/articles>

Articles can be contributed to [staff@net-security.org](mailto:staff@net-security.org)

---

### HOW CAN YOU SPOT A HACKER? by Nicolas Mercier aka Basta

What defines a Hacker? What motivates a Hacker? A majority of people seem to have a vague understanding of what being a Hacker is all about. Is there an underground Hacker community? Is there only one type of Hacker? As far as a definition, I think that there isn't "one" final definition of the word because it's essence is in constant motion and evolution.

Read more:  
< <http://www.net-security.org/text/articles/hacker.shtml> >

---

## Security Software

---

All programs are located at:  
<http://net-security.org/various/software>

---

### SYGATE PERSONAL FIREWALL 4.1 B814

Sygate Personal Firewall is a bi-directional intrusion-defense system for your personal computer. It ensures that your computer is protected from hackers and other intruders while preventing unauthorized programs on your computer from accessing the network. Sygate Personal Firewall makes machines invisible to the outside world. It works on computers connected to a private network or the Internet. This program assures that your business, personal, financial, and other data is safe and secure.

Info/Download:  
< <http://www.net-security.org/various/software/996169363,97521,windows.shtml> >

---

### RETINA 4.02

From the developer: "Retina is a network security scanner. It identifies and fixes potential security holes that exist in your network. Retina can not only figure out known security holes but also new holes in your network. Many new features and functionalities have been added to Retina 4.02. A few of these are: Customizable Reporting, Remote OS Detection, New Audits Wizard, Faster Scans, and much,

much more."

Info/Download:

< <http://www.net-security.org/various/software/996009468,84573,windows.shtml> >

---

## ZONEALARM PRO 2.6

ZoneAlarm Pro automatically blocks known and unknown Internet threats. For home users, small-business owners and corporate employees working remotely, ZoneAlarm Pro offers the highest level of protection and control. It provides comprehensive, customizable settings that let you tailor security controls to your exact needs. Unlike conventional firewalls, ZoneAlarm Pro monitors outgoing application traffic as well as incoming traffic, protecting you from any local applications attempting to use your Internet connection to communicate with the outside world. You have the option to grant and deny access on an per-application basis, customizing the protection for your system. A unique signature integrity check insures that you cannot be fooled by imposters pretending to be a trusted application. ZoneAlarm Pro also offers password protection, automatic mobile PC protection, e-mail attachment protection for 37 different file types, and can control your security by blocking IP addresses that run port scans.

Info/Download:

< <http://www.net-security.org/various/software/996009544,23688,windows.shtml> >

---

## IDA SCRIPT REMOVAL UTILITY

This is in response to the sheer numbers of web server that got pummeled by this new worm. While many people and firms created exploit/checks/Advisories for this Dangerous exploit, we have yet to see a "helping hand" program...until now! Having previously worked at a site with a huge server farm I experienced how painful it can be to go to 175 machines to install a single hot fix. This program will allow you to sit at your desk and simply yank the script mappings from the web server altogether and eliminate some 6 or so vulnerabilities that are associated with Index Services. This is a very simple program that you can use to remove the .IDA and .IDQ script mappings from the root of a web server and from all its sub-web sites. We have included the source code as well as the setup packages (the metautil.dll has to get installed) for your perusal.

Info/Download:

< <http://www.net-security.org/various/software/995708962,27778,windows.shtml> >

---

## BLACKICE AGENT (ISAPI EXTENSION BUG UPDATE)

This release updates BlackICE's intrusion detection capability to detect few new attack signatures, including the one on ISAPI extension overflow.

Info/Download:

< <http://www.net-security.org/various/software/995710203,9841,windows.shtml> >

---

## CYBERSCRUB

Use CyberScrub to protect your privacy and remove all evidence of your online activity with methods that exceed standards set by the US Dept. of Defense. This fine utility provides the tools you need to easily remove every trace of sensitive data from your computer. In addition to performing secure deletion on specific files and folders, CyberScrub includes a handy wizard interface to step through selections that ensure your privacy. Remove history, photos, chatroom conversations, cookies, temp files, and typed URLs for both Netscape and Internet Explorer, as well as user-defined folders and files. This fine protection package can also clear the Windows swap file and Recycle Bin, free disk space, and delete email.

Info/Download:

< <http://www.net-security.org/various/software/995729835,62259,windows.shtml> >

-----  
Defaced archives  
-----

[30.07.2001]

Original: <http://www.securityiss.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/30/www.securityiss.com/>

OS: Windows

Original: <http://www.securitycanada.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/30/www.securitycanada.com/>

OS: Windows

Original: <http://www.digitalsecurity.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/30/www.digitalsecurity.com/>

OS: Windows

[31.07.2001]

Original: <http://www.samsung.com.au/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/31/www.samsung.com.au/>

OS: Windows

Original: <http://www.acer.am/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/31/www.acer.am/>

OS: Windows

Original: <http://www.ford.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/31/www.ford.com/>

OS: Windows

[01.08.2001]

Original: <http://www.alcatel.se/>

Defaced: <http://defaced.alldas.de/mirror/2001/08/01/www.alcatel.se/>

OS: Windows

Original: <http://forum.matrox.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/08/01/forum.matrox.com/>

OS: Solaris

Original: <http://www.alcatel.com.br/>

Defaced: <http://defaced.alldas.de/mirror/2001/08/01/www.alcatel.com.br/>

OS: Windows

Original: <http://www.pfizer.fr/>

Defaced: <http://defaced.alldas.de/mirror/2001/08/01/www.pfizer.fr/>

OS: Windows

[02.08.2001]

Original: <http://www.nokia.co.za/>

Defaced: <http://defaced.alldas.de/mirror/2001/08/02/www.nokia.co.za/>

OS: Windows

Original: <http://www.secrets.co.uk/>

Defaced: <http://defaced.alldas.de/mirror/2001/08/02/www.secrets.co.uk/>

OS: Windows

[03.08.2001]

Original: <http://www.pfizer.se/>

Defaced: <http://defaced.alldas.de/mirror/2001/08/03/www.pfizer.se/>

OS: Windows

Original: <http://www.pfizer.at/>

Defaced: <http://defaced.alldas.de/mirror/2001/08/03/www.pfizer.at/>

OS: FreeBSD

Original: <http://www.chemag.basf.de/>

Defaced: <http://defaced.alldas.de/mirror/2001/08/03/www.chemag.basf.de/>

OS: Windows

[04.08.2001]

Original: <http://www.pepsi-cola.com.cn/>

Defaced: <http://defaced.alldas.de/mirror/2001/08/04/www.pepsi-cola.com.cn/>

OS: Windows

Original: <http://www2.verisign.co.jp/>

Defaced: <http://defaced.alldas.de/mirror/2001/08/04/www2.verisign.co.jp/>

OS: Windows

Original: <http://www.redhat.gr/>  
Defaced: <http://defaced.alldas.de/mirror/2001/08/04/www.redhat.gr/>  
OS: Windows

Original: <http://www.core.tdk.co.jp/>  
Defaced: <http://defaced.alldas.de/mirror/2001/08/04/www.core.tdk.co.jp/>  
OS: Windows

Original: <http://www.cgi.com/>  
Defaced: <http://defaced.alldas.de/mirror/2001/08/04/www.cgi.com/>  
OS: Windows

[05.08.2001]

Original: <http://dp.mercedes-benz.com/>  
Defaced: <http://defaced.alldas.de/mirror/2001/08/05/dp.mercedes-benz.com/>  
OS: Windows

Original: <http://www.epson.co.th/>  
Defaced: <http://defaced.alldas.de/mirror/2001/08/05/www.epson.co.th/>  
OS: Windows

-----  
=====  
Help Net Security T-Shirt available  
=====  
Thanks to our affiliate Jinx Hackwear we are offering you the opportunity  
to wear a nifty HNS shirt :) The image speaks for itself so follow the link  
and get yourself one.  
Get one here: <http://207.21.213.175:8000/ss?click&jinx&3af04db0>  
=====

Questions, contributions, comments or ideas go to:

Help Net Security staff

[staff@net-security.org](mailto:staff@net-security.org)  
<http://net-security.org>  
<http://security-db.com>