

HNS Newsletter  
Issue 71 - 16.07.2001  
<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>

Current subscriber count to this digest: 2635

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

=====  
LANguard Security Event Log Monitor

=====  
LANguard SELM is a network wide event log monitor that retrieves logs from all NT/2000 servers and workstations and immediately alerts the administrator of possible intrusions. Through network wide reporting, you can identify machines being targeted as well as local users trying to hack internal company information. LANguard analyses the system event logs, therefore is not impaired by switches, IP traffic encryption or high-speed data transfer.

Download your evaluation copy from:  
<http://www.net-security.org/cgi-bin/ads/ads.pl?banner=gfitxt>

=====  
General security news  
-----

-----  
**US GOVERNMENT ADMITS SECURITY BLUNDER**

The US Department of Commerce has taken down part of its official website amid fears that sensitive data from companies including Microsoft, Intel and HP has been compromised.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1123753>

#### ANTI-CHILD PORN VIRUS ON THE LOOSE

A new strain of Windows virus tries to weed out perverts by identifying all files on PCs that may contain child pornography, then notifies the British authorities. The "Noped" virus is sent as a VBS (Visual Basic Script) attachment on an email titled: 'Help us all to end illegal child porn now'. Once the attachment is opened the virus will automatically direct itself to the recipient's address book to send itself on. It then scans the PC's hard drive for any JPEG pictures with titles that may indicate child pornography. If the virus locates any such files it will forward samples of them to a list of UK government agencies.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.idgnet.co.nz/webhome.nsf/UNID/88B4DC45FD52DEAFCC256A810010F7C2)

[bin/news.cgi?url=http://www.idgnet.co.nz/webhome.nsf/UNID/88B4DC45FD52DEAFCC256A810010F7C2](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.idgnet.co.nz/webhome.nsf/UNID/88B4DC45FD52DEAFCC256A810010F7C2)

#### CYBERCRIME SKYROCKETS, SAY SECURITY REPORTS

Cybercops say computer crime incidents more than doubled last year, creating a virtual crime wave across computer systems all over the world. More than 21,000 incidents, up from nearly 10,000 in 1999, were reported in 2000 to Carnegie Mellon University's Software Engineering Institute, which tracks online criminal activity in the United States and helps victims. This year's first quarter saw more than 7000 reported incidents.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.thestandard.com/article/0,1902,27731,00.html)

[bin/news.cgi?url=http://www.thestandard.com/article/0,1902,27731,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.thestandard.com/article/0,1902,27731,00.html)

#### STEVE GIBSON PICKS A FIGHT

Security consultant Steve Gibson has posted another DDoS diatribe following a conference call with the Beast of Redmond's security team. In an extremely rare occurrence, however, The Register has been clumped with Microsoft and both received a barracking at his hands. Well, more precisely Thomas C Greene has been clumped with MS. Claiming that his concerns and complaints about XP have fallen on deaf ears, Steve Gibson states: "and thanks to many other loud and equally security-ignorant voices which are attempting to confuse the industry on this topic, Microsoft shows no intention of responding to this now very visible threat" with part of the text hyperlinked to one of our stories.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/20160.html)

[bin/news.cgi?url=http://www.theregister.co.uk/content/55/20160.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/20160.html)

#### TOP 10 SECURITY MISTAKES

People are more careless with computers than perhaps any other thing of value in their lives. The reason is unclear, but observers agree that end users - and even some IT departments - can be pretty dumb when it comes to protecting computers and their contents. Presented in this article are some notable, less than-bright errors that people and IT professionals commit when it comes to computer security.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/itresources/rcstory/0,4167,STO61986_KEY73,00.html)

[bin/news.cgi?url=http://www.computerworld.com/itresources/rcstory/0,4167,STO61986\\_KEY73,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/itresources/rcstory/0,4167,STO61986_KEY73,00.html)

#### THE END OF TRUST AS WE KNOW IT?

It was sure to happen! There has been much said about the fact that PKI solutions, while technically interesting, are operationally challenging. The recent security announcement from Microsoft acknowledging that an errant code-signing certificate is in the wild is a clear call to action for those of us charged with the design, deployment and operation of solid information

security infrastructure. The question of the moment is, "Exactly what should that action be?"

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.scmagazine.com/scmagazine/sc-online/2001/article/026/article.html>

#### THE ENEMY WITHIN

Experts agree that cybercrimes are often the result of a combination of factors that are unique to the modern IT workplace. Although most managers believe that "security is both about risk management and hiring honest people," experts in criminal psychology say the onus is often on managers to take action to prevent current and former employees from lashing out in the form of cybercrime.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/rckey73/story/0,1199,NAV63\\_STO61983,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/rckey73/story/0,1199,NAV63_STO61983,00.html)

#### LINUX AUTHENTICATION USING OPENLDAP, PART TWO

This is the second article of a two-part series devoted to discussing LDAP authentication on Linux. The first installment, offered an overview of LDAP, installing and configuring OpenLDAP, migrating to OpenLDAP and setting up LDAP queries. This installment will look at setting up PAM and NSS for LDAP, securing the root account, some LDAP tools, securing OpenLDAP, OpenLDAP and SSL, and some concerns about OpenLDAP.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/linux/articles/openldap2.html>

#### MICROSOFT TO TAP VERISIGN FOR SECURITY

Microsoft will enlist VeriSign to help provide security for its planned set of Internet services called .Net. Through this deal, VeriSign will provide additional "digital certificates" over the Passport system for certain transactions requiring extra security, such as bank transfers, the companies said.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1003-200-6528869.html>

#### SMOKING MAD OVER POT VIRUS

An annoying but relatively harmless virus that advocates legalizing marijuana is making enemies out of some potential allies: potheads. Unlike Stoned, which appeared a dozen years ago and could corrupt all data on a disk drive, the Marijuana virus doesn't damage victims' PCs. Its payload, which is spread by an e-mail worm and through a Trojan Horse program, sets the infected computer's Internet Explorer browser start page to marijuana.com and places an unmistakable green, palmate leaf in the Windows system tray of an infected PC.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/culture/0,1284,45101,00.html>

#### CHASING THE WIND, EPISODE EIGHT: STILL WATERS

This is the eighth installment in Robert G. Ferrell's popular series, Chasing the Wind. As we left off last time, Douglas continued to be both excited and unnerved by the Bellatrix project and Ian had given himself a scare while defacing a corporate web site. Meanwhile, Bob wrestled with the frustration

of the construction of the new Acme Ailerons complex, which was now behind schedule and over budget. However, it seemed that for one group of shady people, the construction problems were all part of a much larger plan.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/ih/articles/chasing8.html>

#### HOME NETWORK SECURITY

This document gives home users an overview of the security risks and countermeasures associated with Internet connectivity, especially in the context of "always-on" or broadband access services (such as cable modems and DSL). However, much of the content is also relevant to traditional dial-up users (users who connect to the Internet using a modem).

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cert.org/tech\\_tips/home\\_networks.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cert.org/tech_tips/home_networks.html)

#### USING PHP SECURELY

The following article tries to explain how to use PHP on your server in a secure manner. This includes how to safely install it, remove samples and set up security specific options.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securiteam.com/securitynews/5VP041F4UU.html>

#### DEF CON & BLACK HAT BRIEFINGS

If the slot machines get a little screwy this week, casino detectives will have plenty of suspects. Thousands of computer hackers and security experts begin converging in Las Vegas Tuesday for the annual Black Hat Briefings and Def Con convention on computer security. With individuals and corporations increasingly relying on buggy software and the Internet to manage everything from their finances to their personal health records, incidents of malicious hacking continue to increase. More than 7,000 computer security violations were reported in the first three months of this year, more than in all of 1998, according to the CERT Coordination Center, a security research group at Carnegie-Mellon University in Pittsburgh.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsfactor.com/perl/story/11885.html>

#### PROTECTING INFORMATION FROM EXPOSURE (PART III)

So you've done everything you can to prevent information from being exposed while it's in use. Your network is encrypted, you use encrypted drive partitions and encrypted swap file where possible, and you have blocked access to the Internet and removable devices. No matter how hard you try, chances are the data exists somewhere in an unencrypted format that you are not aware of: a temp file, a swap file, or from the original file server itself.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/closet/closet20010711.html>

#### BOOK REVIEW: "SECRETS AND LIES" BY BRUCE SCHNEIER

Security is a fundamental component of doing business in this world. Transactions between businesses, consumers, and governmental organizations--they all depend on ensured data privacy, integrity, and availability to some degree. The common mantra regarding security in the online world seems to be: use encryption. But is that really all there is to it? Is encryption the panacea that it is so often proposed to be? Bruce Schneier emphatically informs us that it

is not. Instead, for Schneier, security is a much larger animal that must be applied at every level of a system. In his book, "Secrets and Lies" Schneier attempts to bring information regarding security and the implications of that security to the masses. Schneier presents this information in a truly engaging manner, and takes care to cover a wide range of security topics.

Link: <http://www.linux.com/enhance/newsitem.phtml?sid=1&aid=12467>

#### CEO OF TROUBLED BALTIMORE TECHNOLOGIES STEPS DOWN

The Internet security software maker Baltimore Technologies PLC said its chief executive, Fran Rooney, had quit in a move analysts said increased the possibility of a takeover of the troubled Irish company.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.iht.com/articles/25675.html>

#### MICROSOFT ADDRESSES ENCRYPTION FLAW IN WIN2K

A flaw in Windows 2000 could allow attackers to read copies of sensitive data that has been encrypted on the computer, Microsoft has acknowledged. The vulnerability stems from a crash-recovery mechanism in the Encrypting File System. In some instances, EFS automatically creates plain-text backups of files as it encrypts or decrypts them. While EFS deletes the backup copies once the original file is successfully encrypted or decrypted, the data may still be present on the drive. This is because Win 2000 does not actually remove deleted data but instead de-allocates it so the space can be used by another file. As a result, an attacker with physical access to the computer could potentially read the deleted data using a low-level disk editor or other tool, Microsoft warned.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/167826.html>

#### SLACKBOT DDOS LAUNCHING TROJAN

Troj/Slackbot is a backdoor Trojan horse which can be configured to connect to any IRC server. When the Trojan connects to an IRC server, it joins a pre configured IRC channel and waits for further commands. The Trojan could be used to launch DDoS (distributed denial of service) attacks by sending a large number of UDP packets to a target host.

Link: <http://www.sophos.com/virusinfo/analyses/trojslack.html>

#### DOS RISK FROM ZIP OF DEATH ATTACKS ON AV SOFTWARE

Claims that anti-virus and content filtering packages may be vulnerable to a denial of service attacks through maliciously constructed compressed archives have generated a heated debate in the security industry. A discussion thread on BugTraq on the subject has prompted security consultants MIS Corporate Defence to issue an alert warning its customers of what it describes as an easy way of bringing networks to their knees.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/56/20322.html>

#### CAN PRIVACY RIGHTS SURVIVE?

When it comes to privacy, ever more intrusive collection technologies are being rolled out, such as online tracking mechanisms, spyware, face recognition systems, location tracking devices and even thermal imaging, a Senate Commerce Committee panel was told today. And, Jason Catlett, president of

Junkbusters.com and a visiting fellow at the Kennedy School of Government at Harvard, said in a written statement that "advances in 'cloaking' technologies are always outstripped by advances in collection technologies, both in capabilities and degree of adoption."

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.internetnews.com/bus-news/article/0,,3\\_799411,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.internetnews.com/bus-news/article/0,,3_799411,00.html)

#### WORMS ARE GETTING SMARTER, EXPERT WARNS

Popular peer-to-peer applications like Napster will quietly nurture the next generation of Internet worms, a computer security consultant says. Most worms take advantage of well-known but uncorrected vulnerabilities in software and operating systems to propagate across the Internet, warns Jose Nazario, a biochemistry graduate student and member of a loosely knit group of computer experts known as Crimelabs. He addressed the fifth annual Black Hat Briefings, a security training conference focusing on malicious intruders, here this week.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.pcworld.com/news/article/0,aid,54904,00.asp>

#### TCP SESSION HIJACKING: A PRIMER

TCP session hijacking is a technique for injecting oneself into a communication you're not meant to be involved in. Not just to listen (watch) the communication but to become an active member.

Link: <http://www.netflood.net/article.php?sid=23&mode=thread&order=0>

#### HARDENING HTACCESS, PART ONE

This article is the first in a three-part series that will provide a way to harden htaccess to make it more stable and lessen the chances of successful brute force attacks. This installment will offer a brief overview of htaccess, particularly why it is prone to attacks by brute force, and a look at a couple of hacking tools and methodologies to which htaccess is particularly susceptible.

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

#### INDUSTRY BODY SLAMS NEW SECURITY BILL

The Computing Technology Industry Association (CTIA) has led a stinging attack on the UK Government's Private Security Issue Bill, claiming that it is yet another burden on IT and network professionals. A spokesman for the CTIA said it would mean that security employees will have to obtain a licence from the Government in order to gain employment.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1123870>

#### WIRELESS NETWORKS WIDE OPEN TO HACKERS

On Thursday, Tim Newsham, a researcher for security firm @Stake, presented the details of weaknesses in the password system of wireless networks that could lead to a break in security in less than 30 seconds. The flaw is the third to be uncovered in the so-called Wired Equivalent Privacy, or WEP, protocol that supposedly secures wireless networks. "WEP is inherently insecure," said Newsham. "So using WEP is essentially just throwing another barrier - and a small one - in front of the attacker."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1003-200-6554365.html>

#### PORTSENTRY

As any administrator knows, a successful network rollout begins and ends with security. No matter how much money is spent on a system with the latest and greatest hardware and software, the system can be rendered worthless if its security is compromised. Unfortunately, keeping up with system security can be tedious. Administrators must stay aware of updates to software as well as the latest system compromise techniques. Due to this difficult task, system security is often not maintained and is lacking in many areas. This is illustrated by the increased number of reports that entail system compromise. This dilemma changed for me when I discovered the freeware tools offered by Psionic Software, Inc. called PortSentry and Logcheck. Within minutes, these tools can be installed and configured to improve system security dramatically. Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://noframes.linuxjournal.com/articles/culture/0028.html>

#### DDOS ATTACKS ON THE RISE - EFNET LATEST TARGET

Efnet, the free-to-use IRC network, has been under fire from DDOS attacks on 12-13 July, resulting in most users being blocked from accessing the service. Efnet's unofficial central Web site, Efnet.org, says that Emory University's IRC server was taken offline from Efnet Tuesday evening, removing one of the mainstays of the IRC network that has been in place for around five years. Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/167870.html>

#### EXORCISE FTP, TELENET AND OTHER EVIL DAEMONS

Telnet and ftp send passwords over the network in clear text that can be easily sniffed. You should replace them with more modern tools such as ssh and scp. SSLtelnet/SSLftp are also available but do not seem to be in such wide use. SSH is a better telnet than telnet - it even handles remote X sessions transparently, letting you ssh into another machine and run X apps there with the display automatically exported to your local X server.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.freeos.com/articles/4314/>

#### FEELING SAFE WITH IT SECURITY DEALS

To IT professionals, the word security generally evokes operational-type thoughts. For instance, there's a need for physical security of the data itself. And there's software-controlled access to the secure network. Then there's security to control access to the organization's order entry and financial systems and to the underlying databases. Now, with the proliferation of Web-based systems, Internet firewall security has become a growing concern.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.itworld.com/Sec/2052/CIO010712security>

#### NEW E-MAIL LIST FOR SECURITY BUGS

According to its founders, three high-profile computer security consultants and researchers, VulnWatch will steer clear of the commercialism and bureaucracy that they claim have degraded two of the most popular computer security lists: Bugtraq and NTBugtraq. "We don't expect 20,000 Bugtraq subscribers to cancel their subscription tomorrow and switch to VulnWatch. But what will give us

success is our speed and the quality of our information," VulnWatch co-founder Steve Manzuik told Newsbytes. Manzuik is joined by Weld Pond (manager of research and development for @Stake) and Rain Forest Puppy (a security consultant and prominent figure in the hacking scene).

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/167891.html>

#### MINIMIZING DOS ATTACKS

J. Oquendo writes: "Halting Denials of service attacks a quick and dirty primer on settings and commands to stop or slow down most Denial of Service attacks when your under the gun. Some of the commands were gathered around the net others I have implemented and tested along the way in the midst of attacks as well as in labs. This is not a document that will describe attacks, what they do, nor how they work. Its merely a doc for the sysadmin or security admin to implement along their networks for better protection."

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

#### ANTI-VIRUS SOFTWARE MAKER SEES GROWING DEMAND

Trend Micro said it had not yet decided how to assess the financial outlook for this year but expects demand for its products to continue to grow. Chief Financial officer Mahendra Negi said although there was a recent industry wide slowdown in spending for products that protect computers and networks from software virus attacks and break-ins, long-term growth prospects should remain intact. "We can say that the need for security software should continue to grow because the value of computer networks continues to grow," Negi told Reuters. "In fact, the percentage of spending by companies should go up as networks become more valuable."

Link: <http://www.japantoday.com/e/?content=news&cat=4&id=43056>

#### DEF CON: HACKERS IN SUITS?

Conference organizers call it the "annual computer underground party for hackers," and Defcon is known as much for its technical content as its beer tinged hijinks. Pranks such as smoke bombs in hotel pools, portions of telephone trucks mysteriously appearing in the convention hall and concrete dumped in toilets have earned Def Con a reputation as a kind of annual hacker bacchanalia. Until now. With little fanfare, Def Con has gradually gone corporate.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/culture/0,1284,45224,00.html>

#### HONEYPOTS

For the best security, hack the hackers, suggest security experts who have spent several months watching malicious intruders break into disguised decoy systems on the Internet. The informal study found it was only two to four days before hackers attacked an unprotected Windows 98 system with its file sharing enabled. Hackers attacked one such system four times in a five-day period. The fastest takeover was 15 minutes, when a hacker broke into a PC running Red Hat Linux 6.2.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.pcworld.com/news/article/0,aid,55165,00.asp>

#### THE SANS INSTITUTE WEB SITE DEFACED

In the early hours of Friday morning, a defacer known as "Fluffi Bunni" defaced the website of SANS. On the defacement, it asks "would you really trust these guys to teach you security?"

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.safemode.org/mirror/2001/07/13/www.sans.org/>

#### INTERNET TOO COMPLEX TO SECURE

When he goes to Washington, D.C. next week to testify before the U.S. Congress on computer and Internet security, Bruce Schneier, the CTO of Counterpane Internet Security, would like to tell them that such efforts are currently done poorly and with the wrong goals. He will also tell Congress that "the Internet is too complex to secure," as he said in a speech on the last day of the Black Hat Briefings security conference.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.nwfusion.com/news/2001/0713intsecure.html>

---

#### Security issues

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

---

#### RED HAT SECURITY ADVISORY - XINETD

A vulnerability has been found in xinetd's string handling.  
Link: <http://www.net-security.org/text/bugs/994715916,67312,.shtml>

#### VARIOUS PROBLEMS IN TREND MICRO APPLLETTRAP

AppletTrap includes some design and implementation flaws, which allow an attacker to easily bypass restrictions set by the product administrator. This can be used by internal users to bypass AppletTrap's restrictions and by authorized web servers to redirect the user to unauthorized web servers.

Link: <http://www.net-security.org/text/bugs/994716015,99445,.shtml>

#### CAYMAN-DSL MODEL 3220-H DOS WITH NMAP

Im running a Cayman-DSL Model 3220-H router with GatorSurf version 5.6.1 (build R0). When I use nmap (from command line or through nessus), the router crashes after a few minutes of the beginning of the scan. Ive recreated this in both SynScan and TCP Connect mode, and even by lowering the number of threads used by nmap down to 1.

Link: <http://www.net-security.org/text/bugs/994716057,90474,.shtml>

#### CHECK POINT FIREWALL-1 RDP BYPASS VULNERABILITY

It is possible to bypass FireWall-1 with faked RDP packets if the default implied rules are being used.

Link: <http://www.net-security.org/text/bugs/994716279,96137,.shtml>

#### CHECK POINT RESPONSE TO RDP BYPASS

Check Point uses a protocol called RDP (UDP/259) for some internal communication between software components (this is not the same RDP as IP protocol 27). By default, VPN-1/FireWall-1 allows RDP packets to traverse firewall gateways in order to simplify encryption setup. Under some conditions, packets with RDP headers could be constructed which would be allowed across a VPN-1/FireWall-1 gateway without being explicitly allowed by the rule base.

Link: <http://www.net-security.org/text/bugs/994716333,17858,.shtml>

#### INSECURE TEMPORARY FILES IN TRIPWIRE

Tripwire opens/creates temporary files insecurely. Insecure temporary files are created at least when scanning the filesystem and updating tripwire database.

Link: <http://www.net-security.org/text/bugs/994716416,34564,.shtml>

#### MESSENGER/HOTMAIL PASSWORDS AT RISK

By sniffing the wire, a malicious user can retrieve the scrambler string and the final hash. then he can start a bruteforce session trying all password combinations with the same scrambler prepended and comparing the resulting hash with this he previously sniffed. (an exhaustive attack). Basically, without any bug, messenger is already vulnerable because of the weak cryptographic scheme it uses.

Link: <http://www.net-security.org/text/bugs/994763415,52471,.shtml>

#### MORE PROBLEMS FOR CAYMAN ROUTERS

try using '}' as a username without a password for cayman routers.

login: } Password:

Terminal shell v1.0

Cayman-DSL Model 3220-H, DMT-ADSL (Alcatel) plus 4-port hub

Running GatorSurf version 5.3.0 (build R1)

{} completed login: user level)

Link: <http://www.net-security.org/text/bugs/994848402,54692,.shtml>

#### FREEBSD 4.3 LOCAL ROOT VULNERABILITY

There is local root compromise in FreeBSD 4.3 due to design flaw which allows injecting signal handlers in other processes.

Link: <http://www.net-security.org/text/bugs/994848512,95292,.shtml>

#### MULTIPLE CGI FLAT FILE DATABASE VULNERABILITY

Numerous CGI's store data, including passwords, in a flat file database, using special characters as field and row delimiters. An attacker may be able to manipulate these databases. While many types of CGI's may be vulnerable, CGI's which allow multiple users to log on, and grant certain users privileged or administrator status, are most likely to be exploitable.

Link: <http://www.net-security.org/text/bugs/994938836,84206,.shtml>

#### MYCIO HTTP SERVER DIRECTORY TRAVERSAL

This web server is restricted to serve files that are located under \winnt\mycio \agent\rmrcache , however it is possible to break out of this by using a specially formatted directory traversal URL. This means that an attacker can connect to the webserver and view and/or download any file that resides on the target box. Due to the fact that the service is running as local system NTFS permissions are redundant.

Link: <http://www.net-security.org/text/bugs/994938943,80186,..shtml>

#### COLD FUSION VULNERABILITY PATCH RELEASED

Macromedia has released a patch that addresses two ColdFusion Server security issues which affect all server versions from 2.0 through 4.5.1 SP2 (all editions).

The security issues were discovered through a routine internal security audit.

The security issues potentially expose read and delete access to files on machines running ColdFusion Server as well as overwriting ColdFusion Server templates with zero byte files. Customers are strongly encouraged to upgrade their servers to ColdFusion Server 5 or install the patch as soon as possible.

The security issues DO NOT affect ColdFusion Server 5.

Link: <http://www.net-security.org/text/bugs/994939051,65038,..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/994939171,49661,..shtml>

#### IBM WINDOWS DB2 DENIAL OF SERVICE

IBM DB2 for Windows (98/NT/2000) run 2 services : db2ccs.exe (listening on port 6790) and db2jds.exe (port 6789). I may be wrong but these services are used to access data remotely and to remotely manage the database. Both can be crashed remotely: just telnet on their port, send one byte and then close the connexion, that's all.

Link: <http://www.net-security.org/text/bugs/994939260,3921,..shtml>

#### CISCO IOS PPTP VULNERABILITY

PPTP implementation using Cisco IOS software releases contains a vulnerability that will crash a router if it receives a malformed or crafted PPTP packet. No special conditions or router configuration is required.

Link: <http://www.net-security.org/text/bugs/995138042,19471,..shtml>

#### VPN-1/FIREWALL-1 FORMAT STRINGS VULNERABILITY

A security issue exists in VPN-1/FireWall-1 version 4.1 whereby a valid firewall administrator connecting from an authorized management client may send malicious data to a management station inside a control connection, possibly preventing proper operation of the management station. This issue exists because some instances of improper string formatting occur in VPN-1/FireWall-1 version 4.1.

Link: <http://www.net-security.org/text/bugs/995138077,78008,..shtml>

## MULTIPLE VULNERABILITIES IN FEW ARCHIVERS

Among them: huge files with high compression ratio are able to fill memory/disk, special device names and special characters in file names, directory traversal (dot-dot bug). Probably, directory traversal is most dangerous among this bugs, because it allows to craft archive which will trojan system on extraction.

Link: <http://www.net-security.org/text/bugs/995138113,72047,.shtml>

---

## Security world

---

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

---

## RAINBOW FORMS JOINT VENTURE IN JAPAN - [10.07.2001]

Rainbow Technologies, Inc., a leading provider of high-performance security solutions for the Internet and eCommerce, and SOFTBANK EC HOLDINGS CORP., a Japanese leader in software distribution and Internet infrastructure solutions, announced a joint venture aimed at becoming the leading supplier of Internet security products in Japan, the largest IT market in Asia and the second largest IT market in the world.

Press release:

< <http://www.net-security.org/text/press/994717224,70811,.shtml> >

---

## ADVANCED NT SECURITY EXPLORER 2.0 RELEASED - [10.07.2001]

Advanced NT Security Explorer (ANTExp) is password security test tool that makes it easy for NT/2000/XP systems administrators to identify and close security holes in their networks. By running a password security test tool like Advanced NT Security Explorer regularly, systems administrators can have peace of mind that the basic lock on their networks is secure. Password hacking is one of the top ten most critical Network security threats. More too often, users like to use simple and easy-to-remember passwords such as repeating characters, simple words, and names. In addition, network administrators are often either too lax or overworked to purge terminated employees from the system, force people to change passwords often or lock out users after a number of failed attempts.

Press release:

< <http://www.net-security.org/text/press/994762406,91479,.shtml> >

Download:

< <http://www.net-security.org/various/software/994768117,83599,windows.shtml> >

---

RAINBOW TECHNOLOGIES TEAMS IKEY 2000 - [10.07.2001]

Rainbow Technologiesä, Inc., (Nasdaq: RNBO), a leading provider of high performance security solutions for the Internet and eCommerce, announced that Rainbow's iKey 2000 Series workstation token has been certified compatible with Computer Associates' software and is "ca smart" with eTrust PKI and eTrust Web Access Control. Rainbow worked closely with Computer Associates International, Inc. (NYSE: CA) to achieve the certification - ca smart - a new Computer Associates brand-building seal of excellence that validates the iKey 2000 series' technical integration with eTrust security solutions. The combination of Rainbow's convenient yet powerful authentication token with Computer Associates' eTrust solutions are ideal for large enterprises demanding the highest level of security.

Press release:

< <http://www.net-security.org/text/press/994762531,2961,.shtml> >

-----

EVIDIAN - NEW ACCESSMASTER PKI MANAGER SOFTWARE - [10.07.2001]

Promising a solution to the complexity of implementing and managing public key infrastructure (PKI) environments essential to secure e-business and enterprise computing, Evidian, a leading vendor of secure e-business management software, announced PKI Manager, an enhancement under version 6.0 of its award-winning AccessMaster enterprise and Internet security management software.

Press release:

< <http://www.net-security.org/text/press/994770346,80279,.shtml> >

-----

RSA CONFERENCE 2001 ASIA OPENS IN SINGAPORE - [11.07.2001]

Making its initial foray into Asia, the RSA Conference 2001 Asia opened at the Singapore International Convention and Exhibition Center in Suntec City, Singapore. Modeled after the successful U.S.-based RSA Conference - the world's largest data security event - RSA Conference 2001 Asia is designed to address the critical e-security and privacy issues facing business, government and the public. With the participation of major industry leaders such as the Singapore Infocomm Development Authority (IDA), the convention is designed to inform, educate and raise e-security issues among key IT professionals, business people, mathematicians and developers in Asia.

Press release:

< <http://www.net-security.org/text/press/994848753,70435,.shtml> >

-----

DSET SELECTS RSA SECURITY - [11.07.2001]

RSA Security Inc., the most trusted name in e-security, announced that DSET Corporation, a leading supplier of software known as electronic-bonding gateways that enable competitive service providers in the telecommunications industry to implement an automated Trading Partner Network, has incorporated RSA BSAFE Crypto-C encryption software into its ezNumberPort system. A TPN plays a critical role in lowering the cost of acquiring customers, reducing the

amount of time required to turn on services for new customers, and minimizing the time required to resolve service outages to ensure higher customer satisfaction and less customer turnover. The ezNumberPort gateway enables communications between competitive service providers and the eight regional Number Portability Administration Centers in the United States and Canada. By incorporating RSA BSAFE encryption technology into its gateway, DSET helps enable secure communications between ezNumberPort and the NPAC.

Press release:

< <http://www.net-security.org/text/press/994848803,83487,.shtml> >

---

#### CARNEGIE MELLON'S CYBERSECURITY CENTER ACQUIRED - [11.07.2001]

RedSiren Technologies Inc. announced that it has signed a definitive agreement to acquire Secure360, the CyberSecurity Center of Carnegie Mellon Research Institute. This acquisition complements and extends RedSiren's managed security monitoring services with Secure360's consulting services. "Carnegie Mellon is a global leader in computer science and computer security. We also are committed to economic development. This purchase is strong evidence that the Pittsburgh region has an emerging cluster of cybersecurity businesses," said Carnegie Mellon President Jared Cohon. Carnegie Mellon, as a shareholder in RedSiren, will be represented on the RedSiren Advisory Board.

Press release:

< <http://www.net-security.org/text/press/994848899,40332,.shtml> >

---

#### 10TH USENIX SECURITY SYMPOSIUM - AUGUST 13-17 - [12.07.2001]

In depth, immediately useful TUTORIALS:

- \* Wireless IP Security and Connectivity
- \* Network Security
- \* Intrusion Detection and Network Forensics
- \* Hacking Exposed: Live!
- \* Cryptographic Algorithms Revealed
- \* VPN Architecture and Implementation

Press release:

< <http://www.net-security.org/text/press/994933693,20389,.shtml> >

---

#### DIGICERF SELECTS VERISIGN - [12.07.2001]

DigiCerf Inc., an online provider of consumer security products, announced that it has selected VeriSign Inc. (Nasdaq:VRSN) to provide authentication and managed digital certificate services to power secure communications products. With VeriSign, DigiCerf plans to issue digital certificates to consumers to enable them to take advantage of the speed and efficiency of conducting secure online communications and transactions. DigiCerf will also use VeriSign's authentication services to establish the identity and authority of consumers requesting digital certificates.

Press release:

< <http://www.net-security.org/text/press/994939449,86633,.shtml> >

---

#### PHOENIX TECH. PARTNERS WITH SECURE COMPUTING - [12.07.2001]

Phoenix Technologies Ltd., the global leader in system software products for connected digital devices, today announced that the company has entered into a long term co-development, co-branding and co-marketing partnership with Secure Computing Corporation, a leading provider of user authentication and access control technology. This partnership will accelerate the adoption of the Phoenix FirstAuthority Trusted Device Infrastructure, a new security model that relies on Phoenix Technologies' 20 plus years at the core of the PC industry to create next generation "trusted devices" and "device-aware" applications.

Press release:

< <http://www.net-security.org/text/press/994939489,82343,.shtml> >

---

#### CA LAUNCHES ETRUST MANAGEMENT SOLUTION - [12.07.2001]

Computer Associates International, Inc., the world's leading provider of eBusiness management solutions, announced the release of the eTrust Management Solution Set, an integrated offering of proven CA technologies that enables large organizations to centrally administer and manage complex security tasks throughout diverse eBusiness environments.

Press release:

< <http://www.net-security.org/text/press/994939602,51292,.shtml> >

---

#### SNAPGEAR'S NEW PRODUCT IN VPN ROUTER MARKET - [12.07.2001]

SnapGear, Inc., a provider of simple, secure and cost effective VPN Internet appliances, announced the establishment of the SnapGear product line. SnapGear plans to market and produce a wide variety of Internet appliances designed for small businesses and branch offices that provide virtual private networking, firewall and network attached storage at a price point below \$300. The SnapGear product line will be sold through the reseller market, with a heavy focus on offering simplicity, security and savings to customers.

Press release:

< <http://www.net-security.org/text/press/994939855,15104,.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)

---

## MITHRIL SECURE SERVER

The Mithril Secure Server does not require the installation of any additional computers or servers. Tovarish installs it for each client as a complete solution that only requires administration of user information.

### Supported Servers

- Any RFC/standards compliant SMTP, IMAP or POP3 server (SSL recommended)
- IMAP/POP3 Servers
- UNIX/Linux: UW-IMAP, Cyrus
- Domino Mail Server
- Exchange
- SMTP Servers
- Exchange
- Qmail
- Sendmail

Read more:

< <http://www.security-db.com/product.php?id=741> >

This is a product of Tovarish, Inc., for more information:

< <http://www.security-db.com/info.php?id=168> >

---

## ETRUST SOLUTIONS

eTrust Solutions provide comprehensive information security solutions to enterprises of any size or geography. Based on best practices, proven and repeatable methods, and leading-edge technology solutions, we maximize the speed and the reliability of your enterprise's security response. And we'll be there to assure that response stays razor-sharp with training, skill transfer and ongoing maintenance services as you need them.

Read more:

< <http://www.security-db.com/product.php?id=482> >

This is a product of Computer Associates International, for more information:

< <http://www.security-db.com/info.php?id=42> >

---

## PRIVILEGE ADMINISTRATOR

Privilege Administrator is a software tool for the system administrator who wants to control, manage and monitor the use of licensed applications in a

network environment. Install the Privilege Administrator tools, even on a small network to enable you to track license usage.

Read more:

< <http://www.security-db.com/product.php?id=179> >

This is a product of Aladdin Knowledge Systems, for more information:

< <http://www.security-db.com/info.php?id=32> >

---

#### 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)

---

#### COMMENTING A FIREWALL by Aleksandar Stancin

The following text deals with a sample firewall, provided for Help Net Security by Mqe. On example of this firewall I'll try to explain some rules and principles behind the concept of building a iptables based firewall.

Read more:

< <http://www.net-security.org/text/articles/ipt.shtml> >

---

#### Security Software

---

All programs are located at:

<http://net-security.org/various/software>

---

#### ATTACKER V3.0

Attacker - A TCP/UDP port listener. You provide a list of ports to listen on and the program will notify you when a connection or data arrives at the port(s). Can minimize to the system tray and play an audible alert. This program is intended to act as a guard dog to notify you of attempted probes to your computer via the Internet.

Info/Download:

< <http://www.net-security.org/various/software/994370131,88182,windows.shtml> >

---

## SCANDET D 1.2

Scandetd is a portscan detector (it can also act as a port flood detector or just a connection logger). It is a daemon that waits for incoming tcp connections and tries to recognize TCP and UDP port scans. Scandetd will also attempt to recognize OS fingerprinting probes. In case of OS probe it will attempt to determine the tool being used, at this point Queso or NMAP. The program can send email to the system administrator.

Info/Download:

< <http://www.net-security.org/various/software/994370532,78654,linux.shtml> >

---

## RATS 1.0

RATS, the Rough Auditing Tool for Security, is a security auditing utility for C and C++ code. RATS scans source code, finding potentially dangerous function calls. The goal of this project is not to definitively find bugs (yet). The current goal is to provide a reasonable starting point for performing manual security audits.

Info/Download:

< <http://www.net-security.org/various/software/994370797,4732,linux.shtml> >

---

## NOTIFYME 1.4.1

Notifyme is a console utility that stays in a background (it isn't a daemon but it doesn't block terminal) and prints a message if a specified login and/or logout occurs. In a resource file (\$HOME/notify.rc by default) you can specify (extended regular expressions are allowed) usernames, hostnames and terminals that should be monitored, optional messages that will be displayed and other options (beep, report logouts etc.) See notifyrc.sample for example. It should be self explanatory. When program starts it reports number of logins and minimum idle time of the users that you specified in a resource file.

Info/Download:

< <http://www.net-security.org/various/software/994371078,33958,linux.shtml> >

---

## FIREWALL TESTER 0.1

The Firewall Tester consists of two simple perl scripts, the client part (ftest.pl) and the listening "daemon" (ftestd.pl). The client injects custom packets, defined in ftest.conf, with a signature in the data part while the daemon listens for such marked packets. The scripts both write a log file wich is in the same form for both scripts. A diff of the two produced files (ftest.log and ftestd.log) shows the packets that were unable to reach the daemon due to filtering rules if the two scripts are runned on hosts placed on two different sides of a firewall.

Of course this is not an automated process, ftest.conf must be crafted

for every different situation. Examples and rules are included in the attached ftest.conf.

Info/Download:

< <http://www.net-security.org/various/software/994515049,10104,linux.shtml> >

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

[09.07.2001]

Original: <http://www.dell.ee/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/09/www.dell.ee/>

OS: Windows

Original: <http://www.orchestrasinfonica.rai.it/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/09/www.orchestrasinfonica.rai.it/>

OS: Windows

Original: <http://www.veterans.org/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/09/www.veterans.org/>

OS: Windows

[10.07.2001]

Original: <http://mediaease.3com.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/10/mediaease.3com.com/>

OS: Windows

[11.07.2001]

Original: <http://www.honda.com.sg/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/11/www.honda.com.sg/>

OS: Windows

[12.07.2001]

Original: <http://www.control-specialists.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/12/www.control-specialists.com/>

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, summer is just around the corner.  
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>