

HNS Newsletter
Issue 69 - 02.07.2001
<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: 2612

Table of contents:

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

BANK CONFIRMS CRACKERS BREAK INTO WEBSITE

The National Australia Bank has confirmed that online vandals broke into and defaced one of the company's Web servers last week. An NAB spokesperson said today the bank detected crackers breaking into and replacing a website's index page on Saturday with a statement denouncing the United States Government and a wellknown website cracker.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://it.mycareer.com.au/breaking/2001/06/25/FFX87XS4DOC.html>

EMAIL LOGIN SECURITY

Most email clients have been configured to check for email automatically every few minutes. This automatic checking involves sending a username and password in clear text from the email client system to the email server. The problem with this is that every time a name and password are sent over the network is an opportunity for an intruder to steal them by using a network sniffer. There are many free and low cost network sniffing tools available for almost all modern operating systems. It's very simple to acquire a sniffer for Windows or several flavors of Unix/Linux. Some vendors even include network sniffers with the operating system.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/emailsecurity20010625.html>

STEVE GIBSON REALLY IS OFF HIS ROCKER

Thomas C. Greene writes: "My recent column ridiculing security specialist Steve Gibson's claim that raw-socket functionality slated for Windows-XP is a major threat attracted more flames than I can hope to post on this page. Briefly, Gibson predicts that the ability of XP's raw sockets to send and forward spoofed packets will result in massive denial of service attacks which no one will be able to stop. I say he's loopy."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/19925.html>

SURVEY: SECURITY PASSWORD PICKS ARE EASY PREY

A computer password survey of British employees highlights what many security experts see as an underrated threat: passwords that are obvious to people or to "cracking" programs widely available on the Internet. The survey, conducted by UK domain registry CentralNic, revealed that nearly half of the workers polled use their own name or a nickname and a third used a favorite sports team or celebrity for their passwords. Security experts say most employees are not aware how easy it is to guess - or more commonly, use a cracking tool - to uncover passwords and gain access to the company network.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsfactor.com/perl/story/11524.html>

DRESS YOUR E-SECURITY IN LAYERS

According to a new white paper on e-commerce security entitled "An Electronic Citadel - A Method for Securing Credit Card and Private Consumer Data in E-Business Sites," military fortification designers in the early 1800s used layers of barriers to weaken and stop attackers, while creating an impenetrable stone fortress at the heart of the citadel. The white paper was written by Tom Arnold, chief technical officer at online security firm CyberSource Corp. "Unfortunately, many of today's e-businesses implement the direct opposite of a citadel," Arnold writes. "This can be viewed as an 'eggshell' security model: hard outer shell, soft in the center."

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://itmanagement.earthweb.com/secu/article/0,,11953_791191,00.html

LEARNING WITH NMAP

Why are scanners so important for the security of networks? Basically because they are essential tools for those who want to attack a system. The preparation of an attack by a cracker could look as follows:

- scan a target machine or selected network

- observe which services are offered and which operating systems runs these services, and work on some well-known vulnerability in any of them
- scan any network or machine, look for a service or operating system (including the checkup of the version) with a known vulnerability.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxfocus.org/English/July2001/article170.shtml)

[bin/news.cgi?url=http://www.linuxfocus.org/English/July2001/article170.shtml](http://www.linuxfocus.org/English/July2001/article170.shtml)

LINUX AUTHENTICATION USING OPENLDAP, PART ONE

LDAP, or Lightweight Directory Access Protocol, is a network protocol that is used for accessing information in an object-oriented database. This is the first of two articles that will discuss a number of issues with LDAP authentication on Linux. In this installment, the author will discuss an overview of LDAP, installing and configuring OpenLDAP, migrating to OpenLDAP and setting up LDAP queries.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/linux/articles/openldap.html)

[bin/news.cgi?url=http://www.securityfocus.com/focus/linux/articles/openldap.html](http://www.securityfocus.com/focus/linux/articles/openldap.html)

EXCHANGE 2000 SERVICE PACK ADDRESSES SECURITY

Microsoft released the first service pack for its Exchange 2000 Server, adding a series of security improvements to a product that has been plagued by security issues in the past month. In addition to patches for that hole, the service pack includes a number of security enhancements, according to Microsoft. They include improvements to antivirus APIs (application programming interfaces) which will allow third-party software vendors to enhance their compatible offerings.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://iwsun4.infoworld.com/articles/hn/xml/01/06/26/010626hnexchange.xml)

[bin/news.cgi?url=http://iwsun4.infoworld.com/articles/hn/xml/01/06/26/010626hnexchange.xml](http://iwsun4.infoworld.com/articles/hn/xml/01/06/26/010626hnexchange.xml)

TWO MACHINES OF THE ICQ NETWORK WERE COMPROMISED

jericho writes: "On June 25, 2001, two machines on ICQ's network were compromised and the web pages defaced. These defacements lead us to wonder if other parts of the network were compromised, possibly allowing access to private ICQ messages, subscriber database or more. The first machine compromised was the ICQ Homepage used to search the ICQ network and user base. The second machine compromised serves an unknown purpose. Originally defaced by MiH, the page is currently defaced by Silver Lords and has no indication of the original content."

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://defaced.alldas.de/mirror/2001/06/25/homepage.icq.com/)

[bin/news.cgi?url=http://defaced.alldas.de/mirror/2001/06/25/homepage.icq.com/](http://defaced.alldas.de/mirror/2001/06/25/homepage.icq.com/)

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://defaced.alldas.de/mirror/2001/06/25/icqgroup01.icq.com/)

[bin/news.cgi?url=http://defaced.alldas.de/mirror/2001/06/25/icqgroup01.icq.com/](http://defaced.alldas.de/mirror/2001/06/25/icqgroup01.icq.com/)

NIPC WARNS OF W32-LEAVES.WORM

The NIPC and FedCIRC have recently received information on attempts to locate, obtain control of and plant new malicious code known as "W32-Leaves.worm" on computers previously infected with the SubSeven Trojan. This new activity, currently under investigation, further increases the importance that all users of Microsoft operating systems take precautions against infection by SubSeven Trojan variants, and, if infected, promptly implement the known procedures to remove the SubSeven infection.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.nipc.gov/warnings/advisories/2001/01-014.htm)

[bin/news.cgi?url=http://www.nipc.gov/warnings/advisories/2001/01-014.htm](http://www.nipc.gov/warnings/advisories/2001/01-014.htm)

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,5093243,00.html>

NEW VERSIONS OF ARIS EXTRACTOR

New versions of the ARIS extractor for both Windows and Unix have been released. ARIS now supports Dragon Network IDS. For those running Dragon NIDS, you may now upload Dragon Sensor logs collected by the Dragon Rider Server and utilize the ARIS analyzer service. Also note that a Sparc Solaris build is now available.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://aris.securityfocus.com/download.asp>

DEFACED.ALLDAS.DE DEFACED

The defaced.alldas.de website was defaced for a short period of time. Quote from the defacement: "As you all visit alldas regularly you will know that hundreds of sites a day get hit by malicious crackers. Defacements are a perfect way to express one's opinion BUT they can cause serious harm as well. As security gets more and more to 'full disclosure' this opens a way for script kiddies to arise. In fact there's nothing wrong with script kids and ./haxoring as long as it is used with caution."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://defaced.alldas.de/mirror/2001/06/26/defaced.alldas.de>
Link: <http://www.alldas.de/?doc=news#11>

PRODUCT BRIEFING: NETWORK SECURITY SUITES

Now is the time to address your information security needs. Why? According to Gartner Group's "Total Cost of Ownership Model for Information Security," if you don't it will cost you 10 times more 10 years from now. Gartner figures the total cost of information security is now, on average, 0.4 percent of a company's revenue. It expects that to accelerate to 44 percent by 2011.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://itmanagement.earthweb.com/itserv/article/0,,11983_792321,00.html

SEALING THE PIPES - SSH

The paradox of the Internet is that it could never have developed without being open. But that same openness makes today's 'Net vulnerable to attacks of all kinds. The Secure Shell (SSH) protocol is one of a number of solutions developed over the past decade to address this problem. SSH, for the uninitiated, is a program that's used to log into another computer over a network, run programs on a remote system and move files between computers. Providing strong authentication and secure transmission over open channels (like the Internet), Secure Shell replaces less-secure terminal programs, such as telnet and rsh.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infosecuritymag.com/articles/june01/features_protocols.shtml

LDAP OVER SSL VULNERABILITY

An attacker could change another user's password for either of two purposes: to cause a denial of service by preventing the other user from logging on, or in order to log into the user's account and gain any privileges the user had. Clearly, the most serious case would be one in which the attacker changed a domain administrator's password and logged into the administrator's account. Windows

2000 is vulnerable.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.microsoft.com/technet/security/bulletin/MS01-036.asp>.

PRIORITY LIST TO COMBAT CYBERCRIME

A top U.S. Department of Justice official told a congressional subcommittee Tuesday that U.S. law enforcers need more resources to combat cybercrime and better laws to simplify the tracing of suspects over the Internet.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://web.lexis-nexis.com/more/cahners-chicago/11407/7305981/3>

ACTIVETEST SECURECHECK

The ActiveTest SecureCheck service is the first security service from Mercury, which had previously been involved in system and application testing, and offers a range of security tests for corporate networks and e-commerce companies.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://iwsun4.infoworld.com/articles/hn/xml/01/06/26/010626hnmerc.xml>

ADSL FIREWALLS: PRODUCTS REVIEWS

The complexity of PC applications and operating systems, and the pervasiveness of networking, have contributed to continual discovery of security weaknesses - which the typical user cannot be expected to follow or understand. Until now the standard tool for defending PCs was the antivirus scanner, the PC personal firewall has also made its debut. Another alternative is the hardware firewall, particularly interesting for protecting groups of machines, or 'always-on' Internet connections, such as ADSL.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/pf_adsl_tests_20010627.html

DOD'S ABC'S OF COMPUTER "SECURITY"

Never use personal diskettes, Zip disks and the like on classified systems. Computers divide files and write them to disk in units called sectors. If the file's last sector is only partially filled, the machine tops it off with data randomly pulled from memory or hard drives - there's no real telling in advance where the information might come from. So writing and saving even your holiday greetings letter on a classified system is a potential disaster. That's why the practice is a security violation.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://cipherwar.com/news/01/defenselink_on_hackers.htm

AOL'S NOTES ON COUPLE OF ICQ DEFACEMENTS

AOL, in an e-mail response to a query about the attack, said it was aware of one community page on ICQ network that had been altered, adding that the defaced page was one of 20,000 pages (hmm). The problem was resolved with a security patch, AOL said. Also the group that did the defacement today attacked one of the AMEX servers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.itworld.com/Sec/2199/CWD010626icqhack/>

HOW TO TRACE STOLEN NOTEBOOKS OVER THE NET

Software which pinpoints the exact location of laptop thieves via the Net is

due to land in Europe by the end of this year. The software, developed by US company zTrace, activates a tracing technology when stolen laptops are connected to the Internet. Computer owners sign up to zTrace, then notify the company if their machine is stolen (a police report must also be submitted). The tracing technology inside the laptop, which zTrace says cannot be detected or uninstalled, is then activated the next time anyone tries to get the notebook online.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/2/20026.html>

WIRELESS DEVICES AND A NEW GENERATION OF VIRUSES

Although malicious code has yet to have a serious impact on any wireless networks, the increasing capacity and popularity of wireless technology indicates that the chances of such an occurrence are increasing. In this article, SecurityFocus writer Josh Ryder examines the current and future states of wireless technology and looks at the likelihood of a viral incident occurring.

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

HOTKEY ATTACK COULD OPEN WINDOWS SECURITY HOLE

Microsoft denied a report that the hotkeys feature in all versions of its Windows operating system can open a serious security hole. But the company invited security mavens to prove it wrong and test the vulnerability themselves. Scott Culp, head of Microsoft's Security Response Center told Newsbytes today that the software firm has been unable to reproduce an attack reported to the company almost three weeks ago by virus writer Matthew Murphy.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/167350.html>

ANALYSIS OF A "FULL" PGP/GPG KEYRING

Crypto fans will be interested in this study of the PGP keyrings available on public servers. M. Drew Streib set out to analyze the "web of trust" which lies behind the PGP keyring structure. Basically, the keyring servers contain individuals' key signatures, which are in turn affirmed - or signed - by other users. This web of trust is based on who signs whose key - who indicates who is trustworthy. Drew's study provides various statistics about the keys and how they connect. The numbers are of interest both from a statistical point of view and for what they indicate about the social structure and connections between people who use PGP.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://dtype.org/keyanalyze/>

FIREWALLS NOT ENOUGH, SAYS SECURITY VENDOR

Firewalls and intrusion detection systems need an extra layer of protection, according to a leading security vendor. Paul Lawrence, European technical director at Top Layer Networks, said it was crucial to build up a picture of the data traffic on a network and track the movements and identities of any intruders by tracing their so-called 'data DNA'. The company has launched a forensic information gathering tool, SecureWatch, which records information about network activity, such as an intruder's destination and source IP addresses, ports and user names.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1123492>

NORTON ANTIVIRUS 2001 AND REGISTRY SETTINGS

Norton Antivirus 2001 has a very obvious and unsafe registry entry that takes it quite simple to disable NAV2001. According to Peter Kruse who found this problem, if the registry key NAV 2001 is changed in value Norton Anti-Virus startup is disabled, leaving users without any protection against viruses when they restart their machine.

Link: <http://www.theregister.co.uk/content/8/19929.html>

JULY 4 VIRUS HOAX THREATENS MP3 FILES

Preying on the guilt - and gullibility - of digital music swappers, an electronic message circulated the Internet today warning of a ticking time bomb planted on the PCs of Napster users. The press release, which was distributed by e-mail and posted in three Usenet discussion groups devoted to music, announced that on July 4th, American Independence Day, computers around the planet will crash and all MP3 music files on them will be obliterated. Rob Rosenberger, operator of a Web site devoted to debunking computer virus myths and hoaxes, said that the MusicPanel press release is "obviously a hoax - and not a very good one. But some people are falling for it."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/167434.html>

FIREWALL APPLIANCES BACK IN VOGUE

Small and medium-size companies last year spent more money on hardware based firewall appliances than on software-based systems, helping WatchGuard Technologies Inc. remain in the No. 1 position in the most competitive segment of the firewall market, according to a new analyst report. The new study by IDC, "Return of the Black Box: Firewall/VPN Security Appliances Unleashed," concludes that for the first time, firewall appliance revenue last year surpassed software based firewall revenue, coming in at \$942.8 million.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/storyba/0,4125,NAV47_STO61758,00.html.html

YOUR BOSS KNOWS YOU'RE READING THIS

Employee privacy in the United States is under siege as old rules for what employers can and cannot monitor give way to a regime of everyday observation, patchy legal protections and conflicting business priorities. Software that pores over intimate e-mail correspondences, tracks worker performance or thwarts employee theft has narrowed the realm of privacy for employees in offices, factories, on the road or telecommuting from home.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,5084025,00.html>

ELIMINATING IDS BABBLE

A recent International Data Corp. (IDC) survey predicts spending on intrusion detection systems will jump nearly 40 percent over the next two years. But there's a problem hampering the effectiveness of IDSes. Simply put, there are as many different IDS applications as there are attack vectors (figuratively speaking, of course). As many organizations have discovered, multiple IDS solutions are needed to monitor different platforms and networks. This diversity inhibits enterprise-wide pooling and correlation of attack data.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infosecuritymag.com/articles/june01/columns_standards_watch.shtml

SSH HITS THE FAN FOR CISCO ON SECURITY

Cisco products, including its PIX firewall, are subject to multiple vulnerabilities in SSH despite the fact problems with the protocol have been known about for almost a year. Cisco issued a notice to customers which warns that by exploiting weaknesses "inherent" in SSH protocol version 1.5 "it is possible to insert an arbitrary commands into an established SSH session". Attackers might also be able to "collect information that may help in brute force key recovery, or brute force a session key", the notice said.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/20044.html>

CHEESE: IF IT'S GOOD (WORM), LET IT BE!

System administrators worldwide recently reported signs that another self spreading program, or worm, had started to infect Linux systems. The worm's existence has given rise to two schools of thought. One, which feels that the worm will help in securing the system while the other is of the opinion that a worm is a worm after all and has to be eradicated. In this article we bring you the arguments put forth by the "cool about Cheese" school.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.freeos.com/articles/4232/>

HACKER WAGES WAR ON THE WAVES

As the US Navy announces a \$4.1bn attempt to secure the Navy Marine Corps Intranet, hackers have issued a warning that Navy websites are next on the list of targets. The five-year project to secure the NMCI, which consists of 350,000 desktops and 200 networks, dispersed around the world, focuses on controlling virus outbreaks and killing malicious code. The server infrastructure for the NMCI will be consolidated into a small number of server farms to minimise the network access points available to attackers. Last year the Navy detected 23,662 hacking attempts on its networks, but since the kick-off of its multi million security efforts, it has spotted only 125 breaches.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1123521>

PKWARE WEB SITE UNZIPPED

Someone yesterday defaced the home page of PKWARE, Inc., makers of the widely used PKZIP archive and compression file utility. Visitors to the site this morning were greeted with a blank white page except for the following text: "first zip your security holes, then files (if there is time left) :P -the Collective-".

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/167467.html>

NEW MEXICO TEEN CHARGED IN NASA COMPUTER ATTACK

Federal authorities have accused an Albuquerque teenager of hacking into a NASA computer at the Ames Research Center in Northern California. Jason Schwab, 18, has been charged with computer abuse and conspiracy to commit computer abuse, according to documents filed in Children's Court in Bernalillo County. NASA officials said the computer system was compromised during the alleged attack in April 2000. They said files

were modified and illegal accounts were added.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.nandotimes.com/technology/story/35745p-582339c.html)

[bin/news.cgi?url=http://www.nandotimes.com/technology/story/35745p-582339c.html](http://www.nandotimes.com/technology/story/35745p-582339c.html)

SECURITY PLANNING PAYS OFF

Experts believe IT managers should spend more time assessing risks and prioritising investment when formulating their security strategies. The issue of security has received a lot of coverage recently following Microsoft's efforts to patch a series of security flaws in its NT technology and the accidental exposure of credit card details on the Consumers' Association Web site. Recent research conducted for IT Week showed that security is the top concern among IT managers.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,s2090331,00.html)

[bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,s2090331,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,s2090331,00.html)

Security issues

All vulnerabilities are located at:

<http://net-security.org/text/bugs>

PERCEPTION LITESERVE MS-DOS VULNERABILITY

When GET requests are made to LiteServe's webserver with the name of the cgi-bin directory as a MS-DOS directory name (eg. cgi-shizznitch=CGI-SH~1 and cgi-bin=CGI-BIN), LiteServe will read the script instead of executing it.

Link: <http://www.net-security.org/text/bugs/993490930,64016,.shtml>

SMBD REMOTE FILE CREATION VULNERABILITY

Insufficient parameter validation and unsafe default configuration make numerous systems running samba SMB file sharing daemon vulnerable to remote attacks.

Link: <http://www.net-security.org/text/bugs/993491092,62072,.shtml>

SAMBA SECURITY BUGFIX RELEASED

A serious security hole has been discovered in all versions of Samba that allows an attacker to gain root access on the target machine for certain types of common Samba configuration.

Link: <http://www.net-security.org/text/bugs/993491321,65260,.shtml>

DEBIAN SECURITY ADVISORY - SAMBA UPDATE

Michal Zalewski discovered that samba does not properly validate NetBIOS names from remote machines. By itself that is not a problem, except if Samba is configure to write log-files to a file that includes the NetBIOS name of the remote side by using the `%m` macro in the `log file` command. In that case an attacker could use a NetBIOS name like `../tmp/evil`. If the log-file was set

to "/var/log/samba/%s" samba would them write to /var/tmp/evil.

Link: <http://www.net-security.org/text/bugs/993491363,11055,..shtml>

EXTREMAIL REMOTE FORMAT STRING

eXtremail is a free integrated pop3/smtpd mail daemon for Linux (x86), although it is free it is closed sourced software. It has been found that the majority of the newer versions are vulnerable to a remotely exploitable format string condition.

Link: <http://www.net-security.org/text/bugs/993491539,52009,..shtml>

CFINGERD LOCAL VULNERABILITY

When the option ALLOW_LINE_PARSING is set (and this seems to be by default, each user can specify what cfingerd returns to the querying person. The problem is situated in util.c, line 181-182:

```
while((line[pos] != ' ') && (!done)) {  
command[newpos] = line[pos];
```

This while loop does not check whether the end of the buffer "command" has been reached. (The buffer is 80 chars long.) This leads to a buffer overflow. Even more alarming is that it can lead to a local root exploit, because cfingerd is allowed to run as root, and it doesn't seem to drop the privileges when it performs that while loop.

Link: <http://www.net-security.org/text/bugs/993491644,8175,..shtml>

ASP SOURCE CODE RETRIEVED WITH UNICODE EXTENSION

With Unicode there are many ways the asp extension can be encoded. On FAT file systems some of them will not be recognized as an ASP script by IIS and executed on the server but instead IIS will disclose the source code of the script.

Link: <http://www.net-security.org/text/bugs/993491887,61571,..shtml>

CERBERUS FTP SERVER 1.X REMOTE DOS ATTACK

Cartel security team has found a buffer overflow in the Cerberus FTP server, which means that an attacker can execute a denial of service attack against it. This attack will crash the server, without any error. FTP service is then unavailable.

Link: <http://www.net-security.org/text/bugs/993544067,32779,..shtml>

MULTIPLE VULNERABILITIES IN WEB-SHOP 1C

Multiple vulnerabilities in web-shop 1C: Arcadia, in module tradecli.dll

1. Show path scripts directory.

Exploit: <http://host/scripts/tradecli.dll?template=nonexistfile>

Will show error message, witch consist full path to work dir (usually /scripts).

2. Read any file from drive.

tradecli.dll - language interpreteter of 1C: Arcadia. It will work up file, pointed in template, interpret tags, bigining with underline symbol (example, <_include...>), all the rest read without changes, put in ASCIIZ line and then print as result. Path, pointed in variable template, will not work up for special symbols, so you can get direcopy up (..\) and the full path to file, you may read file only from drive, where lies work directory of tradecli.dll.

Exploit: <http://host/script/tradecli.dll?template=..\..\..\..\path\to\file>

Reading of binary files will be embarrassing, because data after 0 symbol will'nt print.

3. Crash ISAPI-applications (DoS)

Opening of files: com1, com2, etc. Windows NT application will crash, that will

crash all application (1C: Arcadia), consequently site.

Link: <http://www.net-security.org/text/bugs/993544144,14223,..shtml>

RED HAT - FTP IPTABLES VULNERABILITY IN 2.4 KERNEL

A security hole has been found that does not affect the default configuration of Red Hat Linux, but it can affect some custom configurations of Red Hat Linux 7.1. The bug is specific to the Linux 2.4 kernel series. Aside from the fix, countless bugfixes have been applied to this kernel as a result of code-audits by the MC project of the Stanford University and others.

Link: <http://www.net-security.org/text/bugs/993544380,9329,..shtml>

CALDERA OPENLINUX - BUFFER OVERFLOW IN FETCHMAIL

In previous versions of fetchmail, there were buffer overflows when handling mail messages with very long header fields. This hole could theoretically be exploited remotely by sending messages with such headers.

Link: <http://www.net-security.org/text/bugs/993624385,54137,..shtml>

CALDERA OPENLINUX: SAMBA REMOTE ROOT PROBLEM

There is a file overwrite vulnerability in the log facilities of the Samba filesharing package which can be used by a remote attacker to overwrite system files and to gain root access. This requires a specific logging entry to be set. Caldera OpenLinux is not vulnerable to this problem in its default configuration, because it does not include a default configuration file for Samba and the sample configuration we ship has logging commented out.

Link: <http://www.net-security.org/text/bugs/993624483,15348,..shtml>

SECURITY ISSUES WITH ICECAST VERSION 1.3.7

Remote DoS attack - If the server has enabled the http-server file streaming support, a malicious client can perform a DoS remotely. Http-server file streaming support is not enabled by default, but is enabled by altering variable "staticdir" in the configuration-file "icecast.conf". The DoS causes an "Application Error" in Windows, thus crashing the Icecast-server completely. The DoS is caused by adding an extra "/" or "\" behind the requested mp3-file.

Folder traversal exploit - Mp3-files residing outside the Web catalog can be accessed by replacing ascii-values for each ".", thus using "%25%25/" instead of "../" will walk one folder downward.

Link: <http://www.net-security.org/text/bugs/993624582,45811,..shtml>

SOLARIS 8 LIBSLDAP BUFFER OVERFLOW

The library implementing LDAP naming services on Solaris 8, libslldap, contains a buffer overflow in the initialization code. While parsing the environment variable LDAP_OPTIONS, a fixed size buffer is used to store its contents which can be of any length. This is a straightforward buffer overflow and exploitable in conjunction with privileged programs that use the library. Such programs include passwd, yppasswd, nispasswd, sendmail, and chkey. The library is only found on Solaris 8 systems. On vulnerable systems the buffer overflow can lead to a local root compromise.

Link: <http://www.net-security.org/text/bugs/993624639,3362,..shtml>

MANDRAKE LINUX SECURITY - KDELIBS UPDATE

A problem exists with the kdesu component of kdelibs. It created a world

readable temporary file to exchange authentication information and delete it shortly after. This can be abused by a local user to gain access to the X server and could result in a compromise of the account that kdesu would access.

Link: <http://www.net-security.org/text/bugs/993814879,13280,.shtml>

ORACLE 8I SQLNET HEADER VULNERABILITY

A vulnerability in the Oracle implementation of the TNS (Transparent Network Substrate) over Net8 (SQLNet) protocol allows a remote user to mount a denial of service attack against any Oracle service that relies upon the protocol, including the TNS Listener, Oracle Name Service and Oracle Connections Manager.

Link: <http://www.net-security.org/text/bugs/993814984,66666,.shtml>

VULNERABILITY IN ORACLE 8I TNS LISTENER

The Oracle 8i TNS (Transparent Network Substrate) Listener is responsible for establishing and maintaining remote communications with Oracle database services. The Listener is vulnerable to a buffer overflow condition that allows remote execution of arbitrary code on the database server under a security context that grants full control of the database services and, on some platforms, full control of the operating system. Because the buffer overflow occurs prior to any authentication, the listener is vulnerable regardless of any enabled password protection.

Link: <http://www.net-security.org/text/bugs/993815080,96695,.shtml>

VIRUSWALL 3.51 SMTPSCAN.DLL BUFFER OVERFLOW

A buffer overflow vulnerability was found in some administrative programs, smtpscan.dll, of InterScan VirusWall for Windows NT. It allows a remote user to execute an arbitrary command with SYSTEM privilege.

Link: <http://www.net-security.org/text/bugs/993815196,49200,.shtml>

VIRUSWALL 3.51 HTTPSAVEC*P.DLL BUFFER OVERFLOW

A buffer overflow vulnerability was found in some administrative programs, smtpscan.dll, of InterScan VirusWall for Windows NT. It allows a remote user to execute an arbitrary command with SYSTEM privilege.

Link: <http://www.net-security.org/text/bugs/993815278,45442,.shtml>

MACOS PERSONAL WEB SHARING DoS

The problem this time is that when File Sharing is set to check PWS logins, on a about 300char password the system freezes. This problem could be bigger, cause Macintosh File sharing passwords cannot be longer than 8 chars and many apps support File Sharing to controls logins, ie the same users that are set in FS control panel can access the specified service. I have tested it on a PPC 9500, OS 9.1z1, PWS v. 1.5.5. I have not had the tme to test it with any other server apps which have File Sharing control-access. If anyone has one nearby and will test it let me know.

Link: <http://www.net-security.org/text/bugs/993815347,35725,.shtml>

SUSE SECURITY ANNOUNCEMENT ON SAMBA

Michal Zalewski discovered that a remote attacker can write to files owned by root if the samba config file /etc/smb.conf contains the %m macro to specify

the logfile for logging access to the samba server. The %m macro substitutes the NetBIOS name - improper validation of this name allows an attacker to write to any file in the system. SuSE Linux distributions do not ship a default /etc/smb.conf config file that contains the %m macro. Therefore, SuSE distributions are not vulnerable to the bug in the out-of-the-box state.
Link: <http://www.net-security.org/text/bugs/993917652,27600,.shtml>

EXPIRED HTTP PASSWORDS & 302 HTTP STATUS CODE

A combination of expired HTTP password (for instance an expired SecurID token code) and the 302 HTTP status code (Moved Temporarily) breaks the IE authentication mechanism. After the password expires and the user tries to retrieve a page, IE prompts the user for the new password. However, if IE receives a 302 Status Code instead of a 200 after a successful HTTP authentication, it attempts to retrieve the moved page with the OLD (cached and expired) password. When this fails, IE prompts the user for the new password, retrieves this page successfully, but then goes on to retrieve the next page (or page element) with the old password. This behavior repeats ad infinitum, or until the SecurID token is locked because ACE detects a replay or simultaneous authentication attack. This was tested with IE 5.5, but is anecdotally known to break all MS version 5 browsers.

Link: <http://www.net-security.org/text/bugs/993918072,47719,.shtml>

Security world

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

----- WHALE COMMUNICATIONS TEAMS WITH RSA SECURITY - [25.06.2001]

Whale Communications, a leader in Air Gap technology, announced that it has joined the RSA Secured Partner Program to support interoperability between the e-Gap product line and RSA SecurID(R) authentication technology. As part of the program, the e-Gap System's family of products has been awarded "RSA Secured RSA SecurID Ready" certification, signaling its compatibility with RSA Security's authentication technology. The RSA Secured certification lets organizations know that the e-Gap System's product line is compatible with RSA Security's market-leading security products and technologies.

Press release:
< <http://www.net-security.org/text/press/993492328,11222,.shtml> >

----- MEXICO'S LARGEST BANK DEPLOYS PGP E-PPLIANCE - [25.06.2001]

PGP Security, a division of Network Associates, is now shipping the PGP 1000

e-ppliance, a new network security appliance capable of securing up to a gigabit of data throughput per second. The PGP 1000 e-ppliance extends PGP Security's industry leading security appliance product line as one of the most comprehensive offerings in the marketplace, which protects the increasing levels of network traffic resulting from the expanding use of the Internet as a strategic business platform.

Press release:

< <http://www.net-security.org/text/press/993546451,53007,.shtml> >

IDENTIX LAUNCHES ITS FIRST ITRUST OFFERING - [25.06.2001]

Identix Incorporated, the leading biometric provider of end-to-end security solutions, launched its first itrust offering, a comprehensive access control security platform that safeguards information sharing and data transfer on open wired and wireless networks. Based on the three most important aspects of security - authentication, authorization and administration - itrust offers a comprehensive solutions platform for today's wired and wireless business. itrust is offered as a service on either a transaction-based or annual licensing model.

Press release:

< <http://www.net-security.org/text/press/993546595,96463,.shtml> >

NETEYE NOW SHIPPING VERSION 2.0 OF HAWKEYE - [26.06.2001]

NetEye Corp. announced that it is now shipping version 2.0 of its HawkEye NextGen Fraud & Security Management solution, a comprehensive fraud and security management solution for IP & Next Generation Networks. First introduced in June of 2000, HawkEye NextGen Fraud is part of the HawkEye NextGen Product suite - a modular and flexible suite of carrier-grade business and management solutions for IP & Next Generation Networks. These networks transmit both voice and multi-service data over a packet-based network.

Press release:

< <http://www.net-security.org/text/press/993624100,3347,.shtml> >

MDD INC. ANNOUNCES PASSWORD BOUNCER 1.0 - [27.06.2001]

MDD Inc. a provider of software for automating Windows NT and Windows 2000 system administration today announced availability of Password Bouncer 1.0. For Windows NT/2000 system and security administrators concerned about unauthorized access to user accounts, MDD's Password Bouncer is a centralized management console for preventing vulnerable passwords from being used by employees and contractors. Unlike existing security products, Password Bouncer defeats hackers by using their own methods in the on-going battle to protect your network.

Press release:

< <http://www.net-security.org/text/press/993723081,23138,.shtml> >

MDD INC. LAUNCHES TRUSTED ENTERPRISE MANAGER 4.0 - [28.06.2001]

MDD Inc. a provider of software for automating Windows NT and Windows 2000 system administration announced availability of Trusted Enterprise Manager 4.0. For Windows NT/2000 and Microsoft Exchange system administrators concerned about reducing the complexity of managing operations in the Microsoft Enterprise, MDD's TEM 4.0 is a centralized console for simplifying and automating routine tasks. Unlike existing system management products, TEM combines rich task automation and secure delegation along with a SQL repository resulting in lower cost of ownership, greater administrator accountability and enhanced network security.

Press release:

< <http://www.net-security.org/text/press/993723147,99419,.shtml> >

U.S. GOVERNMENT'S NSF SELECTS NETSEC - [28.06.2001]

NETSEC, a global provider of managed information security services, announced it has been awarded a multi-year contract to provide its services to the National Science Foundation (NSF), the U.S. government agency responsible for promoting research and education projects in science and engineering. NSF's investments total more than \$3.3 billion per year in almost 20,000 research and education projects. NETSEC's experience in the federal sector will assist NSF in their federal information technology compliance efforts.

Press release:

< <http://www.net-security.org/text/press/993724130,22246,.shtml> >

NORMAN ROLLS OUT SUITE OF SECURITY SOLUTIONS - [28.06.2001]

Norman Data Defense Systems, a specialist in the field of data security, announced that it is now offering a suite of information security solutions that are designed specifically to meet the needs of the small business market. Norman's Small Business Suite features Norman's top-rated anti-virus product, Norman Virus Control 5 (NVC 5), Norman Personal Firewall (NPF), and Norman Privacy. "We're pleased to offer a suite of security products that addresses the special needs of small businesses," stated Hank Dugan, President and Chief Executive Officer of Norman Data Defense Systems, the North American subsidiary of Norman ASA. "

Press release:

< <http://www.net-security.org/text/press/993724188,34598,.shtml> >

RSA SECURITY SECURES REUTERS CONTENT DELIVERING - [28.06.2001]

RSA Security Inc., the most trusted name in e-security, announced that Reuters, the global information, news and technology group, has selected RSA BSAFE encryption software to secure the streaming flow of financial information issued by its Internet Finance Platform. Specifically, Reuters has licensed the software

to secure the communication between its end-users and Reuters' Streaming System (RSS), an application providing real-time, streaming financial content over the Internet.

Press release:

< <http://www.net-security.org/text/press/993724393,14829,.shtml> >

UNCOMPROMISED \$100,000 E-SECURITY CHALLENGE - [29.06.2001]

Secure Computing reiterated that its e-Security Challenge will be retired at the close of the Black Hat and DEFCON Conferences in Las Vegas, July 15, 2001. The contest was originally launched almost one year ago at the Black Hat 2000 conference with a \$10,000 reward for the first person to crack the e-Security Challenge site. At the RSA Conference in April 2001, the reward was raised to \$50,000, and has increased one cent per second until recently, when the maximum award of \$100,000 was reached. As yet, no one has claimed the award.

Press release:

< <http://www.net-security.org/text/press/993815555,81834,.shtml> >

IBM ANNOUNCES AN ENTERPRISE PRIVACY ARCHITECTURE - [29.06.2001]

IBM today unveiled a comprehensive Enterprise Privacy Architecture (EPA) to address the complex privacy challenges facing 21st century businesses, governments and other organizations. The patent-pending EPA provides a road map for privacy management and solutions to help companies protect customer, employee and partner information.

Press release:

< <http://www.net-security.org/text/press/993918317,85879,.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

GATEWAY GUARDIAN PROFESSIONAL EDITION

Gateway Guardian Professional Edition meets and exceeds the needs of the average business on the Internet today. With high-end, fully flexible firewalling functionality, Professional Edition provides complete control over who can

access and who can leave the network. Taking it one step further, it also allows complete control over the type of traffic going through the Internet gateway.

Read more:

< <http://www.security-db.com/product.php?id=726> >

This is a product of Merilus Inc, for more information:

< <http://www.security-db.com/info.php?id=102> >

DIGITAL SIGNATURE AUTHENTICATION

Increasingly countries around the world are recognizing the need to use digital signatures in electronic transactions. Certicom's Digital Signature Authentication Solution is an integrated, key enabling technology that reduces the risk of conducting online business transactions. It is a robust, standards-based authentication method using Certicom technology and products that delivers trusted, fast user authentication and authorization through the combined use of digital signatures and existing account database environments.

Read more:

< <http://www.security-db.com/product.php?id=364> >

This is a product of SmartLine, for more information:

< <http://www.security-db.com/info.php?id=108> >

XACTA COMMERCE TRUST

Xacta is developing a series of increasingly more powerful risk assessment and mitigation tools. In fact, Xacta's product development organization is working aggressively to incorporate a host of additional security regulations and industry best practices to better address the needs of the federal and commercial marketplaces.

Read more:

< <http://www.security-db.com/product.php?id=752> >

This is a product of Xacta Corporation, for more information:

< <http://www.security-db.com/info.php?id=172> >

Featured article

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

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

XATO COMMENTARY ON NSA SECURITY DOCUMENTS by .sozni

The National Security Agency (NSA) released a series of documents on the subject of Windows 2000 security. Since we at Xato focus so much on IIS security, we were anxious to see what the world's most elite intelligence agency had to share. As we dove into the IIS document we were quite disappointed with what we found. Instead of discovering a wealth of information in these recently unclassified documents, we found a largely inadequate and sometimes incorrect security guide.

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

Defaced archives

[25.06.2001]

Original: <http://homepage.icq.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/06/25/homepage.icq.com/>
OS: Windows

Original: <http://icqgroup01.icq.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/06/25/icqgroup01.icq.com/>
OS: Windows

Original: <http://icqgroups.icq.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/06/25/icqgroups.icq.com/>
OS: Windows

Original: <http://www.borland.com.tw/>
Defaced: <http://defaced.alldas.de/mirror/2001/06/25/www.borland.com.tw/>
OS: Windows

Original: <http://www.samsung.it/>
Defaced: <http://defaced.alldas.de/mirror/2001/06/25/www.samsung.it/>
OS: Windows

Original: <http://atwnt302.external.hp.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/06/25/atwnt302.external.hp.com/>
OS: Windows

Original: <http://atwnt401.external.hp.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/06/25/atwnt401.external.hp.com/>
OS: Windows

[26.06.2001]

Original: <http://www.burgerking.co.uk/>
Defaced: <http://defaced.alldas.de/mirror/2001/06/26/www.burgerking.co.uk/>
OS: Windows

Original: <http://defaced.alldas.de/>
Defaced: <http://defaced.alldas.de/mirror/2001/06/26/defaced.alldas.de/>
OS: Linux

Original: <http://list.creative.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/06/26/list.creative.com/>
OS: Windows

[27.06.2001]

Original: <http://download.asia.creative.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/06/27/download.asia.creative.com/>
OS: Windows

Original: <http://www.service.medical.philips.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/06/27/www.service.medical.philips.com/>
OS: Windows

Original: <http://www.axi.americanexpress.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/06/27/www.axi.americanexpress.com/>
OS: Windows

[28.06.2001]

Original: <http://www.goodyear.se/>
Defaced: <http://defaced.alldas.de/mirror/2001/06/28/www.goodyear.se/>
OS: Windows

Original: <http://www.canon.es/>
Defaced: <http://defaced.alldas.de/mirror/2001/06/28/www.canon.es/>
OS: Windows

Original: <http://www.zyxel.at/>
Defaced: <http://defaced.alldas.de/mirror/2001/06/28/www.zyxel.at/>
OS: Windows

[29.06.2001]

Original: <http://www.gemini.goodyear.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/06/29/www.gemini.goodyear.com/>
OS: Windows

Original: <http://cle-mlcnd.europe.creative.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/06/29/cle-mlcnd.europe.creative.com/>
OS: Windows

Original: <http://www.samsung.at/>
Defaced: <http://defaced.alldas.de/mirror/2001/06/29/www.samsung.at/>
OS: Windows

Original: <http://www.hyundai.ch/>
Defaced: <http://defaced.alldas.de/mirror/2001/06/29/www.hyundai.ch/>
OS: Windows

[30.06.2001]

Original: <http://www.nec.cl/>
Defaced: <http://defaced.alldas.de/mirror/2001/06/30/www.nec.cl/>
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
<http://net-security.org>
<http://security-db.com>