netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 31

August 4, 2006

Table of Contents

Product Focus

WinArp.exe – Arpd is a daemon that listens to ARP (Address Resolution Protocol) requests and answers for IP addresses that are unallocated. WinArpd in conjunction with our next product, netVigilance WinHoneyd, will be able to populate the unallocated address space in a production network with virtual honeypots. With DHCP allocated IP addresses, it is possible that Arpd interferes with the DHCP server by causing Honeyd to reply to pings that the DHCP server uses to determine if an address is free.

This Week in Review

Black Hats turns into Black eye for Cisco again, Hurray : Microsoft open about security improvements in Vista, New RFID Password already cloned, Ajax gives Hackers new venues, Apple joins Microsoft in releasing 26 Patches, Google Starts warning users about their bad links.

Enjoy reading & Stay safe

Call or email netVigilance to get an update on SecureScout.
(503) 524 5758 or sales@netVigilance.com

Top Security News Stories this Week

- **Black Hat: Unpatched flaw revealed in Cisco firewall**

Cisco just can't seem to make it through the Black Hat USA conference unscathed. On Wednesday a security researcher showed how an unpatched vulnerability in the

company's PIX firewall appliances that could allow outside attackers to gain access to corporate networks.

On the final slide of his presentation on VoIP security, Hendrik Scholz, a developer with Freenet Cityline disclosed a technique for bypassing the firewalls, according to an audio recording of the talk obtained by IDG News.

"You can open up whatever port you want... and access internal servers from the outside," he said "It's really easy to do and we're talking to Cisco about how to get it fixed."

By now Black Hat is old hat for Cisco.
networkworld

Full Story :
http://www.networkworld.com/news/2006/080406-black-hat-unpatched-flaw-revealed.html

❖ Hackers Tip Hat to Windows Vista Security

At the Black Hat conference in Las Vegas, Microsoft gave a full day of briefings on technical aspects of Windows Vista, detailing how it has changed its approach in areas such as networking, the Internet Explorer browser, and how the operating system handles memory. It was an unusual effort by the company to demonstrate progress on the security front.

When a group of Microsoft Corp. employees first attended the Black Hat hacker convention in the late 1990s, the company's security reputation was so bad that one of them says the experience was like constantly hearing people criticize his mother. Apparently, things have changed.

Members of the Black Hat audience responded to Microsoft's briefings on Windows Vista security Thursday not with hostility but with polite interest. The real test won't come until after Windows Vista's retail release next year, but several people said Microsoft appears to have made the operating system more secure.
Newsfactor Network

Full Story :
http://www.newsfactor.com/story.xhtml?story_id=010000CESRTU&page=1

❖ How to clone the copy-friendly biometric passport

So easy the manual tells you that you can do it

At Black Hat yesterday, security consultant Lukas Grunwald of German company DN-Systems demonstrated the cloning of a biometric passport, observing beforehand to Wired that the "whole passport design is totally brain damaged." But should we be surprised? Not exactly, because that's precisely what it says on the tin.

Grunwald boned-up on ICAO (International Civil Aviation Organisation) documentation, bought an ePassport reader and reading software, read a passport (German, but other ePassports would do the trick too), then cloned it. We should however be clear about

what he has done here - he hasn't cracked anything, but he has brought the fundamental flakiness of the ePassports that are now shipping to wider attention. People will no doubt be appalled, but they could just as easily have been appalled some considerable distance back in the production process because that really is what it says on the tin.

The ICAO documentation Grunwald consulted is publicly available, and explains the detail of the various levels of security of the ePassport system, the baseline level being something not unadjacent to zero. For standard ePassports including chip and facial biometric the ICAO assumption is that an open passport can be taken as the bearer's acceptance that the passport is willingly being made available for the data to be read, ICAO's intent here being to duplicate as closely as possible the inherent Ts & Cs of traditional passport inspection systems. But the ePassport is RFID, and therefore vulnerable to skimming and eavesdropping (i.e. being read by a concealed reader and/or having the transaction between passport and 'official' reader snooped on.

Two mechanisms will be used in ePassports to impede this; first, there is the 'tinfoil hat', a mesh of metal in the cover that blocks access to the chip when the passport is closed, and second the machine-readable zone (MRZ) of the passport. The MRZ is designed to be read visually when the passport is open, and this is then compared to the copy of the MRZ held on the chip. If the two match, then the data on the chip can be read.
The Register

Full Story :
http://www.theregister.co.uk/2006/08/04/cloning_epassports/

- **Cybercrooks add Ajax coding to bag of hacking tricks**

LAS VEGAS — The hot new technology behind slick Web pages has suddenly become the hot new tool for cybercriminals.
The technology, Ajax coding and Web tools, enables popular websites such as Google Maps (GOOG) and MySpace.com (NWS) to come alive. It is also the technology behind Windows Live, the slate of cutting edge online services Microsoft has begun testing.

But hackers and cybercrooks have discovered that Ajax can be tweaked in myriad ways. By corrupting one of the dozens of data exchanges Ajax handles while loading a Web page, a hacker can take over control of the PC.

At the giant Black Hat cybersecurity conference here, talks on what kind of Ajax attacks to expect and how to defend against them drew large audiences.

"Ajax has introduced a huge attack surface," says Billy Hoffman, lead engineer at Web security specialist SPI Dynamics. "Ajax works under the covers to make websites really responsive, but criminals can just as easily use it under the covers to do some bad stuff."
USA today

Full Story :
http://www.usatoday.com/tech/news/computersecurity/hacking/2006-08-04-ajax-attack-usat_x.htm

- **Apple Patches 26 Security Flaws**

Apple has released a security update that repairs 26 vulnerabilities in its OS X operating system and bundled applications.

Of the patched security holes, 17 could expose the user to an arbitrary code execution.

Four of the remaining vulnerabilities could lead to disclosure of confidential information, two could cause an application to crash. A local user in three cases could exploit a flaw to gain additional user rights.
Bios Magazine

Full Story :
http://www.biosmagazine.co.uk/article.php?id=3909

- **Google Warning Users About Badware Links**

Users who like to use Google to find things like cracks or license key generators are now receiving the online equivalent of a finger wagged in the face, as Google has started to warn people who click on certain search result links that the destination may be dangerous.

Hunting on Google for links to websites containing less-than-legal ways of circumventing software protection has long been a popular practice for certain people. These links frequently lead to sites hosted outside the United States, in places like Russia and other countries.
SecurityProNews

Full Story :
http://www.securitypronews.com/news/securitynews/spn-45-20060804GoogleWarningUsersAboutBadwareLinks.html

New Vulnerabilities Tested in SecureScout

- **13387 Oracle Database Server - RPC component unspecified vulnerability (jul-2006/DB18)**

An unspecified vulnerability in the RPC component may allow a remote attacker to compromise system integrity and availability.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **High**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
MISC: http://www.red-database-security.com/exploits/oracle-sql-injection-oracle-dbms_export_extension.html

CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
MISC: http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
CERT-VN:VU#932124
URL:http://www.kb.cert.org/vuls/id/932124
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2006-3702

❖ 13388 Oracle Database Server - RPC component unspecified vulnerability (jul-2006/DB19)

An unspecified vulnerability in the RPC component may allow a remote attacker to compromise system integrity and availability.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **High**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
MISC: http://www.red-database-security.com/exploits/oracle-sql-injection-oracle-dbms_export_extension.html
CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
MISC: http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
CERT-VN:VU#932124
URL:http://www.kb.cert.org/vuls/id/932124
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111

URL:http://secunia.com/advisories/21111

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2006-3702

❖ 13389 Oracle Database Server - Semantic Analysis component unspecified vulnerability (jul-2006/DB20)

An unspecified vulnerability in the Semantic Analysis component may allow a remote attacker to compromise system integrity and availability.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **High**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
MISC: http://www.red-database-security.com/exploits/oracle-sql-injection-oracle-dbms_export_extension.html
CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
MISC: http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
CERT-VN:VU#932124
URL:http://www.kb.cert.org/vuls/id/932124
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2006-3702

❖ 13390 Oracle Database Server - Statistics component SQL Injection vulnerability (jul-2006/DB21)

An SQL Injection vulnerability in the Statistics component may allow a remote attacker

to compromise system integrity and availability.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **High**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
BUGTRAQ:20060718 Oracle Database - SQL Injection in SYS.DBMS_STATS [DB21]
URL:http://www.securityfocus.com/archive/1/archive/1/440453/100/0/threaded
BUGTRAQ:20060718 Oracle Database - SQL Injection in SYS.DBMS_UPGRADE [DB22]
URL:http://www.securityfocus.com/archive/1/archive/1/440447/100/0/threaded
MISC: http://www.red-database-security.com/advisory/oracle_sql_injection_dbms_stats.html
MISC: http://www.red-database-security.com/advisory/oracle_sql_injection_dbms_upgrade.html
CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
MISC: http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2006-3705

❖ 13391 Oracle Database Server - Upgrade & Downgrade component SQL Injection vulnerability (jul-2006/DB22)

An SQL Injection vulnerability in the Upgrade & Downgrade component may allow a remote attacker to compromise system integrity and availability.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **High**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
BUGTRAQ:20060718 Oracle Database - SQL Injection in SYS.DBMS_STATS [DB21]
URL:http://www.securityfocus.com/archive/1/archive/1/440453/100/0/threaded
BUGTRAQ:20060718 Oracle Database - SQL Injection in SYS.DBMS_UPGRADE [DB22]
URL:http://www.securityfocus.com/archive/1/archive/1/440447/100/0/threaded
MISC: http://www.red-database-security.com/advisory/oracle_sql_injection_dbms_stats.html
MISC: http://www.red-database-security.com/advisory/oracle_sql_injection_dbms_upgrade.html
CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
MISC: http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2006-3705

❖ 13392 Oracle Database Server - XMLDB component unspecified vulnerability (jul-2006/DB23)

An unspecified vulnerability in the XMLDB component may allow a remote attacker to compromise system integrity and availability.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **High**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
MISC: http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863

URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2006-3700

❖ 13393 Oracle Database Server - OCI component Buffer Overflow vulnerability (jul-2006/DBC01)

A Buffer Overflow vulnerability in the OCI component may allow a remote attacker to compromise system integrity and availability.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **High**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
MISC: http://www.red-database-security.com/exploits/oracle-sql-injection-oracle-dbms_export_extension.html
CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
MISC: http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
CERT-VN:VU#932124
URL:http://www.kb.cert.org/vuls/id/932124
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2006-3702

❖ 13394 Oracle Database Server - RPC component Buffer Overflow vulnerability (jul-2006/DBC02)

A Buffer Overflow vulnerability in the RPC component may allow a remote attacker to compromise system integrity and availability.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **High**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
MISC: http://www.red-database-security.com/exploits/oracle-sql-injection-oracle-dbms_export_extension.html
CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
MISC: http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
CERT-VN:VU#932124
URL:http://www.kb.cert.org/vuls/id/932124
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2006-3702

❖ 13395 Oracle Database Server - RPC component Buffer Overflow vulnerability (jul-2006/DBC03)

A Buffer Overflow vulnerability in the RPC component may allow a remote attacker to compromise system integrity and availability.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **High**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
MISC: http://www.red-database-security.com/exploits/oracle-sql-injection-oracle-dbms_export_extension.html
CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-

updates/cpujul2006.html
MISC: http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
CERT-VN:VU#932124
URL:http://www.kb.cert.org/vuls/id/932124
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2006-3702

❖ 13396 Oracle Database Server - RPC component Buffer Overflow vulnerability (jul-2006/DBC04)

A Buffer Overflow vulnerability in the RPC component may allow a remote attacker to compromise system integrity and availability.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **High**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
MISC: http://www.red-database-security.com/exploits/oracle-sql-injection-oracle-dbms_export_extension.html
CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
MISC: http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
CERT-VN:VU#932124
URL:http://www.kb.cert.org/vuls/id/932124
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2006-3702

New Vulnerabilities found this Week

libTIFF Multiple Vulnerabilities

"Denial of Service"

Some vulnerabilities have been reported in libTIFF, which can be exploited by malicious people to cause a DoS (Denial of Service) or potentially compromise a vulnerable system.

The vulnerabilities are caused due to various heap and integer overflows when processing TIFF images and can be exploited via a specially crafted TIFF image.

Successful exploitation allows crashing applications linked against libTIFF and may also allow execution of arbitrary code.

References:
http://rhn.redhat.com/errata/RHSA-2006-0603.html

GnuPG "parse_comment" Denial of Service Vulnerability

"Denial of Service"

Evgeny Legerov has reported a vulnerability in GnuPG, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an input validation error in parse_packet.c when handling certain message packets. This can be exploited to cause GnuPG to consume large amounts of memory or crash via an overly long comment length in a message packet.

This can further be exploited to cause an integer overflow, which leads to possible memory corruption and crashes GnuPG.

The vulnerability has been reported in version 1.4.4. Prior versions may also be affected.

References:
http://lists.immunitysec.com/pipermail/dailydave/2006-July/003354.html

Mac OS X Security Update Fixes Multiple Vulnerabilities

"Execute arbitrary code"

Apple has issued a security update for Mac OS X, which fixes multiple vulnerabilities.

1) An error in the AFP server within the handling of users' search results can be exploited by malicious users to gain knowledge of the names of files and folders for which the user performing the search has no access to.

Successful exploitation requires that file sharing is enabled.

2) An integer overflow error in the AFP server may be exploited by an authenticated user to execute arbitrary code with system privileges.

Successful exploitation requires that file sharing is enabled.

3) An error in the AFP server where the reconnect keys for file sharing sessions are stored world-readable can be exploited by local users to access files and folders with the privileges of another user.

Successful exploitation requires that file sharing is enabled.

4) An error in the AFP server caused due to an unchecked error condition can be exploited to crash the AFP server by sending a specially crafted invalid AFP request.

Successful exploitation requires that file sharing is enabled.

5) An error in Bom's compression state handling may be exploited to cause a heap corruption by tricking a user into opening a specially crafted corrupted ZIP archive.

Successful exploitation may allow execution of arbitrary code.

NOTE: This can be exploited automatically via the Safari browser if the "Open safe files after downloading" setting is enabled.

6) A boundary error in bootpd can be exploited to cause a stack-based buffer overflow by sending a specially crafted BOOTP request.

Successful exploitation may allow execution of arbitrary code with system privileges, but requires that bootpd is enabled (not enabled by default).

7) An error in the processing of dynamic linker options in privileged applications may be exploited by local users to influence the behavior of privileged applications by specifying options which causes output to standard error.

8) An error in the dynamic linker may be exploited by local users to specify paths used when loading libraries into an privileged application.

Successful exploitation may allow execution of arbitrary code with escalated privileges.

9) Various errors exist in the fetchmail utility.

10) An input validation error when extracting a file with the "-N" flag using "gunzip" makes it possible to have a file extracted to an arbitrary location outside the current directory via directory traversal attacks.

A race condition when setting file permissions has also been reported.

11) An error in the processing of corrupted Canon RAW images can be exploited to cause a buffer overflow by tricking a user into viewing a specially crafted Canon RAW image.

Successful exploitation may allow execution of arbitrary code.

12) An integer overflow error in the processing of corrupted Radiance images may be

exploited to execute arbitrary code by tricking a user into viewing a specially crafted Radiance image.

13) An error in the processing of corrupted GIF images can be exploited to cause an undetected memory allocation failure by tricking a user into viewing a specially crafted GIF image.

Successful exploitation may allow execution of arbitrary code.

14) An integer overflow error in the processing of corrupted GIF images may be exploited to execute arbitrary code by tricking a user into viewing a specially crafted GIF image.

15) An error exists in the download validation of safe files in the LaunchServices where certain files containing HTML may incorrectly be classified as safe. This may be exploited to execute arbitrary HTML and script code in a user's browser session in context of the local domain.

NOTE: This can be exploited automatically via Safari if the "Open safe files after downloading" option is enabled.

16) An error exists in OpenSSH which is caused due to the authentication process hanging when processing login requests by non-existing users. This can be exploited to enumerate valid user accounts or cause a DoS (Denial of Service) via a large amount of login requests.

Successful exploitation requires that remote login is enabled.

17) A design error in the Telnet client when handling the NEW-ENVIRON command can be exploited to gain knowledge of the session variables for a user, who has an open connection to a malicious Telnet server.

18) An error when processing HTML documents can be exploited to access a previously deallocated object.

Successful exploitation may allow execution of arbitrary code, but requires that the user is tricked into visiting a malicious web site.

19) Some errors in the processing of corrupted TIFF images can be exploited to cause buffer overflows (TIFF tag handling, TIFF PixarLog decoder, and TIFF NeXT RLE decoder).

Successful exploitation may allow execution of arbitrary code, but requires that the user is tricked into viewing a specially crafted TIFF image.

References:
http://docs.info.apple.com/article.html?artnum=304063

McAfee SecurityCenter Unspecified Code Execution Vulnerability
“Execution of arbitrary code”

eEye Digital Security has reported a vulnerability in various McAfee products, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an unspecified error in the SecurityCenter when web pages are rendered.

Successful exploitation allows execution of arbitrary code when a user visits a malicious web site.

The vulnerability affects versions 4.3 through 6.0.22.

References:
http://ts.mcafeehelp.com/faq3.asp?docid=407052
http://www.eeye.com/html/research/upcoming/20060719.html

MySQL MERGE Table Privilege Revoke Bypass

"Bypass certain security restrictions"

Peter Gulutzan has reported a vulnerability in MySQL, which can be exploited by malicious users to bypass certain security restrictions.

The vulnerability is caused due to a design error in the user privilege verification for MERGE tables. This can be exploited to keep access to a table via an in advance created MERGE table even after the privilege has been revoked for the table.

References:
http://dev.mysql.com/doc/refman/4.1/en/news-4-1-21.html
http://dev.mysql.com/doc/refman/5.0/en/news-5-0-24.html

VMware ESX Server Multiple Vulnerabilities

"Gain knowledge of potentially sensitive information; Conduct cross-site request forgery attacks"

Corsaire has reported some vulnerabilities in VMware ESX Server, which can be exploited to gain knowledge of potentially sensitive information or conduct cross-site request forgery attacks.

1) When changing passwords using the management interface, the GET request containing the password in clear text is logged to a world-readable file.

2) The management interface uses a proprietary session ID format containing authentication credentials encoded in base64. If malicious people get hold of the session cookies, it's possible to gain knowledge of the user account and password.

3) The management interface allows users to perform certain actions via HTTP GET requests without performing any validity checks to verify the user's request. This can be exploited to change a user's password when user visits a malicious web site while logged in.

Safari "KHTMLParser::popOneBlock()" Memory Corruption

A vulnerability has been discovered in Safari, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an error in the "KHTMLParser::popOneBlock()" function. This can be exploited to cause a memory corruption via a script element in a div element redefining the document body.

Successful exploitation may allow execution of arbitrary code.

The vulnerability has been confirmed in version 2.0.4 (419.3). Other versions may also be affected.

References:
http://browserfun.blogspot.com/2006/07/mobb-31-safari-khtmlparserpoponeblock.html

Vulnerability Resource
Check out this compendium of links and up-to-the minute information about network security issues. Their claim to be the 'security portal for information system security professionals' is well founded. http://www.infosyssec.org/infosyssec/

Thank You
Thanks for sifting through another great edition of the ScoutNews. We hope we captured a flavor for the week and gave you just enough information on newly found vulnerabilities to keep you up-to-date. To subscribe or unsubscribe, contact us at ScoutNews@netVigilance.com.

About SecureScout
SecureScout is a leading vulnerability scanner and management tool developed and marketed worldwide by NexantiS Corporation.
SecureScout is a trademark of NexantiS Corporation.
netVigilance, Inc. is a partner of NexantiS and an authorized distributor of SecureScout.

For any inquiry about SecureScout by:
Customers in America and Northern Europe contact us at info@netVigilance.com
Customers in France, Italy, Spain, Portugal, Greece, Turkey, Eastern Europe, Middle East, Africa and Asia/Pacific, contact NexantiS at info-scanner@securescout.net