netVigilance

ScoutNews Team **February 17, 2006**
2006 Issue # 7

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Olympics website attacked from within, FBI chief calls business on hacker silence, Sony flap stirs rootkit discussions at DHS and Skype may avoid wiretapping.

Stay secure out there.

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

Top Security News Stories this Week

- **Olympic Hacker thwarted**

A consultant working for the Olympics organizing committee, threatened to launch an attack against their internal network, was detained by police.

The now former-consultant apparently gained access to network segments where he wasn't allowed.

Associated Press

Full Story :
http://www.washingtonpost.com/wp-dyn/content/article/2006/02/13/AR2006021300387.html

- **FBI boss urges business to report cyber-crimes**

Speaking at the RSA conference in San Jose this week; FBI Director Robert Mueller stressed the importance of breaking the "code of silence" that most businesses resort to when they become victims of cyber-crimes.

Citing consumer sensitivity as the primary driver, Mueller noted that the predominant policy of keeping quiet only benefits the criminals.

Mercury News

Related Links :
http://www.mercurynews.com/mld/mercurynews/business/technology/13887708.htm
http://www.esecurityplanet.com/trends/article.php/3585611

❖ Feds consider ban on Rootkits

Thomas Hesse said in his now infamous remark to a reporter at NPR; Most people don't even know what a rootkit is, so why should they care about it?' Well Mr. Hesse, it is obvious to this reporter that people do care and what's more; the people who don't care unless we care now care: the politicians.

Now that Sony has done us all the service of clearly defining what a rootkit is; the US Department of Homeland Security (DHS) is recommending that the use of rootkits be outlawed. (At least now Sony will have to fund better lobbying activities here in the US – *Ed*.)

E-Commerce Times

Full Story :
http://www.ecommercetimes.com/story/LBe1OYa4z9dJwW/Sony-Incident-Leads-Government-to-Consider-Rootkit-Ban.xhtml

❖ Does Skype negate wiretapping?

Unlike conventional VOIP transmissions; Skype calls are encrypted using 256-bit keys, making crecking virtually impossible. According to Skype they do not provide a "back-door" for government wiretaps. (I think that history will show us how the chips are going to fall on this one – *Ed*.)

ASSOCIATED PRESS

Related Links :
http://www.thejournalnews.com/apps/pbcs.dll/article?AID=2006602170382

New Vulnerabilities Tested in SecureScout

- **14711 W32/Zafi.d@MM Worm (Registry Check)**

This mass-mailing worm arrives in an email message with one of the following extentions: ZIP, CMD, PIF, BAT or COM.

This new variant contains the following characteristics:

Contains its own SMTP engine to construct outgoing messages.

Spoofs the From: address

Harvests target email addresses from the victim machine.

Outgoing email message body is either in Hungarian or English.

Displays p2p worm behaviour.

Shuts down security services.

The worm copies itself to directories on the C: drive containing one of the following strings:

share
upload
music

It copies itself using the below filenames:

winamp 5.7 new!.exe
ICQ 2005a new!.exe

** Further symptoms:

The worm drops the following files to the %windir%\system32 folder:

C:\WINNT\system32\ .EXE - 11,745 bytes
C:\WINNT\system32\
C:\WINNT\system32\Norton Update.exe - 11,745 bytes
C:\WINNT\system32\ .DLL - (worm zipped up)
C:\s.cm - 20,552 bytes (winzip dll module)

It creates a registry key, so the file gets executed every time the machine starts:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
\CurrentVersion\Run "Wxp4" = C:\WINDOWS\SYSTEM32\Norton Update.exe

It creates the following registry key to store information of the worm:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wxp4

TCP port 8181 is opened on the infected system.

** Method of Infection

This worm does not use any exploit code in order to execute the mail attachment automatically. A user has to doubleclick on an infected attachment or a file shared via P2P to infect the machine.

For machines where the worm has overwritten binaries associated with AV or firewall software, it would be very easy for a user to mistakenly execute the worm.

** Mail Propagation

This virus constructs messages using its own SMTP engine. Target email addresses are harvested from files on the victim machine.

Harvested addresses are stored in five files in the system32 folder using random names and the file extension .DLL. For example:

c:\WINDOWS\SYSTEM32\ckolieqt.dll
c:\WINDOWS\SYSTEM32\fktnxowp.dll
c:\WINDOWS\SYSTEM32\gczomkgr.dll
c:\WINDOWS\SYSTEM32\hgtmrsvo.dll

The body of the email sent by the worm are in the form of Christmas greetings. Like previous variants, the worm sends itself out in different languages depending on the Top Level Domain (TLD) of the recipient's address. For example, a user with a .COM mail address, will receive the English mail body, while someone with an .DE Mail address will receive the German body.

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

References:

http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=130371

CVE Reference: GENERIC-MAP-NOMATCH

❖ 14712 W32/Rontokbro.D@mm Worm (Registry Check)

**Characteristcs

This mass-mailing worm arrives as an attachment with the filename: Kangen.exe

Contains its own SMTP engine to construct outgoing messages.

Attempts to find SMTP server by adding the following prefixes to domain names: smtp, mail, ns1.

Spoofs the From: address

Harvests target email addresses from the victim machine.

Makes coppies of itself on the local machine.

Adds various registry entries so that it will be executed on startup.

**Symptoms

When W2.Rontokbro.D@mm is executed, it performs the following actions:

Copies itself to the following Files:

%UserProfile%\Local Settings\Application Data\csrss.exe
%UserProfile%\Local Settings\Application Data\inetinfo.exe
%UserProfile%\Local Settings\Application Data\lsass.exe
%UserProfile%\Local Settings\Application Data\services.exe
%UserProfile%\Local Settings\Application Data\smss.exe
%UserProfile%\Local Settings\Application Data\winlogon.exe
%UserProfile%\Start Menu\Programs\Startup\Empty.pif
%UserProfile%\Templates\WowTumpeh.com
%Windir%\eksplorasi.pif
%Windir%\ShellNew\bronstab.exe
%System%\[user name]'s Setting.scr

Creates the directory:

%UserProfile%\Local Settings\Application Data\Bron.tok-[X]-[Y]

Where [X],[Y] are two random numbers.

Overwrites C:\Autoexec.bat with the following text:

"pause"

Adds the value:

"Bron-Spizaetus" = "%Windir%\ShellNew\bronstab.exe"

to the registry subkey:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that it runs every time Windows starts.

Adds the value:

"NoFolderOptions" = "1"

to the registry subkey:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

Adds the value:

"Hidden" = "0"
"ShowSuperHidden" = "0"
"HideFileExt" = "1"

to the registry subkey:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\explorer\advanced

Adds the values:

"DisableRegistryTools" = "1"
"DisableCMD" = "0"

to the registry subkey:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System

Adds the value:

"Tok-Cirrhatus" = "%UserProfile%\Local Settings\Application Data\smss.exe"

to the registry subkey:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

so that it runs every time Windows starts.

Adds the value:

"Shell" = "Explorer.exe %Windir%\eksplorasi.pif"

to the registry subkey:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

so that it runs every time Windows starts.

Adds a task to the Windows scheduler to execute the following file at 5:08 PM every day:

%Windir\Tasks\At1.job

**Method Of Infection

Executing the attached file: Kangen.exe

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

References:

http://securityresponse.symantec.com/avcenter/venc/data/w32.rontokbro.d@mm.html

CVE Reference: GENERIC-MAP-NOMATCH

❖ 14713 W32/WORM_DELODER.A Worm (Registry Check)

This worm uses the valid utility, PSEXEC.EXE, to connect to remote machines. It attempts to log on to the machines as administrator using several passwords listed in its body. It connects via TCP port 445 and drops a copy of itself as Dvldr32.exe and a backdoor program as INST.EXE on accessible machines.

The backdoor component, installs several legitimate network and remote access tools to allow remote users to access and manipulate affected machines.

This worm, which runs on Windows 2000 and XP, attempts to remove the following network shares:

* ADMIN$
* IPC$
* C$
* D$
* E$
* F$

**Symptoms

This worm runs on Windows 2000, XP, and the Server 2003 family. It drops copies of itself as the file Dvldr32.exe on target machines.

When executed on the said platforms, it extracts the valid network utility, PSEXEC.EXE by SysInternals, into the directory where it is executed.

It creates the following registry entry so that it executes at Windows startup:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\Run

messnger = &ltWorm Path>\Dvldr32.exe

*Where &ltWorm Path> is the location where this worm is executed.

To prevent multiple instances of itself in memory, it creates a unique mutex named "testXserv".

This worm uses TCP port 445, also known as the Microsoft-DS port, to connect to remote machines. It first generates random IP address and then attempts to connect to remote machines on the IP addresses using any of the following 85 hard-coded passwords.

This worm attempts to connect to all 255 possible IP addresses on a subnet that it has generated. For example, if it generates the subnet 10.10.10.XXX, it attempts to connect to remote machines with IP addresses from 10.10.10.0 to 10.10.10.255.

If the logon attempt is successful, it drops and executes a read-only copy of itself on the target machine in the Windows system folder as Dvldr32.exe. It also drops and executes a read-only backdoor program file, inst.exe, in the same folder and in the

following hard-coded folders:

* \%s\C$\WINNT\All Users\StartMenu\Programs\Startup
* \%s\C\WINDOWS\Start Menu\Programs\Startup
* \%s\C$\Documents and Settings\All\Users\Start\Menu\Programs\Startup

Note: %s is the network name of the remote target machine.

Dropping the file, INST.EXE, ensures that the backdoor component, which is detected as BKDR_DELODER.A, is executed at startup on the remote machine.

This worm continuously executes this network propagation routine while it is resident in memory.

Using the PSEXEC.EXE tool, the worm attempts to remove the following hidden network shares:

* ADMIN$
* IPC$
* C$
* D$
* E$
* F$

On certain samples of this worm, the dropped file INST.EXE has been found to be actually non-malicious and works as installer of a legitimate Remote Administration tool.

Upon execution of the non-malicious INST.EXE, it drops the following files, all of which are normal files:

* dialer.exe (this file name varies)
* raddrv.dll
* AdmDll.dll

It does not create autostart registry entries.

Dialer.exe, better known as RAdmin.21 (Remote Administrator server v2.1), is actually a server component of a legitimate Remote Administrator Tool. This tool works on Windows 2000 and XP platform and runs using "Remote Administrator service" as its service name.

Once this service is active, a remote user running the client component is able to see what is displayed on the infected machine. In addition, all mouse movements and keystrokes are transferred directly to the remote system.

The other files, raddrv.dll and AdmDll.dll, are normal components of the tool and function solely for its processes and installation.

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

References:

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FDELODER%2EA&VSect=P

CVE Reference: GENERIC-MAP-NOMATCH

❖ 16123 Cumulative Security Update for Internet Explorer (MS06-004/910620) (Remote File Checking)

A remote code execution vulnerability exists in Internet Explorer because of the way that it handles Windows Metafile (WMF) images. An attacker could exploit the vulnerability by constructing a specially crafted WMF image that could potentially allow remote code execution if a user visited a malicious Web site, opened or previewed an e-mail message, or opened a specially crafted attachment in e-mail. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Note that this vulnerability in Internet Explorer is separate from the vulnerabilities addressed in Windows in MS05-053 and MS06-001.

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

References:

Original advisory:
http://www.microsoft.com/technet/security/Bulletin/MS06-004.mspx

Other references:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0020
* MLIST:[funsec] 20060110 Another WMF flaw without a Microsoft patch
* URL:http://linuxbox.org/pipermail/funsec/2006-January/002828.html
* CONFIRM:http://www.microsoft.com/technet/security/advisory/913333.mspx
* CERT:TA06-045A
* URL:http://www.us-cert.gov/cas/techalerts/TA06-045A.html
* CERT-VN:VU#312956
* URL:http://www.kb.cert.org/vuls/id/312956
* BID:16516
* URL:http://www.securityfocus.com/bid/16516
* FRSIRT:ADV-2006-0469
* URL:http://www.frsirt.com/english/advisories/2006/0469
* SECUNIA:18729
* URL:http://secunia.com/advisories/18729

CVE Reference: CVE-2006-0020

❖ 16124 Vulnerability in Windows Media Player Could Allow Remote Code Execution (MS06-005/911565) (Remote File Checking)

A remote code execution vulnerability exists in Windows Media Player because of the way that it handles processing bitmap files. An attacker could exploit the vulnerability by constructing a malicious bitmap file (.bmp) that could potentially allow remote code execution if a user visited a malicious Web site or viewed a malicious e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, significant user interaction is required to exploit this vulnerability.

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

References:

Original advisory:

http://www.microsoft.com/technet/security/Bulletin/MS06-005.mspx

Other references:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0006

* CERT:TA06-045A

* URL:http://www.us-cert.gov/cas/techalerts/TA06-045A.html

* CERT-VN:VU#291396

* URL:http://www.kb.cert.org/vuls/id/291396

CVE Reference: CVE-2006-0006

❖ 16125 Vulnerability in Windows Media Player Plug-in with Non-Microsoft Internet Browsers Could Allow Remote Code Execution (MS06-006/911564) (Remote File Checking)

A remote code execution vulnerability exists in the Windows Media Player plug-in for non-Microsoft Internet browsers because of the way the Windows Media Player plug-in handles a malformed EMBED element. An attacker could exploit the vulnerability by constructing a malicious EMBED element that could potentially allow remote code execution if a user visited a malicious Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

References:

Original advisory:
http://www.microsoft.com/technet/security/Bulletin/MS06-006.mspx

Other references:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0005
* IDEFENSE:20060214 Microsoft Windows Media Player Plugin Buffer Overflow Vulnerability
* URL:http://www.idefense.com/intelligence/vulnerabilities/display.php?id=393
* CERT:TA06-018A
* URL:http://www.us-cert.gov/cas/techalerts/TA06-018A.html
* CERT-VN:VU#692060
* URL:http://www.kb.cert.org/vuls/id/692060

CVE Reference: CVE-2006-0005

❖ 16126 Vulnerability in TCP/IP Could Allow Denial of Service (MS06-

007/913446) (Remote File Checking)

A denial of service vulnerability exists that could allow an attacker to send a specially crafted IGMP packet to an affected system. An attacker could cause the affected system to stop responding.

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

References:

Original advisory:
http://www.microsoft.com/technet/security/bulletin/ms06-007.mspx

Other references:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0021
* CERT:TA06-018A
* URL:http://www.us-cert.gov/cas/techalerts/TA06-018A.html
* CERT-VN:VU#839284
* URL:http://www.kb.cert.org/vuls/id/839284
* BID:16645
* URL:http://www.securityfocus.com/bid/16645
* FRSIRT:ADV-2006-0576
* URL:http://www.frsirt.com/english/advisories/2006/0576
* SECUNIA:18853
* URL:http://secunia.com/advisories/18853

CVE Reference: CVE-2006-0021

❖ **16127 Vulnerability in Web Client Service Could Allow Remote Code Execution (MS06-008/911927) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Windows processes Web Client requests that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

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

References:

Original advisory:
http://www.microsoft.com/technet/security/bulletin/ms06-008.mspx

Other references:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0013
* CERT-VN:VU#388900
* URL:http://www.kb.cert.org/vuls/id/388900
* BID:16636
* URL:http://www.securityfocus.com/bid/16636
* SECUNIA:18857
* URL:http://secunia.com/advisories/18857

CVE Reference: CVE-2006-0021

❖ 16128 Vulnerability in the Korean Input Method Editor Could Allow Elevation of Privilege (MS06-009/901190) (Remote File Checking)

A privilege elevation vulnerability exists in the Windows and Office Korean Input Method Editor (IME). This vulnerability could allow a malicious user to take complete control of an affected system. For an attack to be successful an attacker must be able to interactively logon to the affected system.

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

References:

Original advisory:
http://www.microsoft.com/technet/security/Bulletin/ms06-009.mspx

Other references:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0008
* BUGTRAQ:20060215 Security advisory: Windows IME Vulnerability (MS06-009)
* URL:http://www.securityfocus.com/archive/1/archive/1/425141/100/0/threaded
* MISC:http://www.ryanstyle.com/alert/my/5/ms06_009_eng.html

CVE Reference: CVE-2006-0008

❖ 16129 Vulnerability in PowerPoint 2000 Could Allow Information Disclosure (MS06-010/889167) (Remote File Checking)

An Information Disclosure vulnerability exists in PowerPoint. An attacker who successfully exploited this vulnerability could remotely attempt to access objects in the Temporary Internet Files Folder (TIFF) explicitly by name. Note that this vulnerability would not allow an attacker to execute code or to elevate their user rights directly, but it could be used to produce useful information that could be used to try to further compromise the affected system.

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

References:

Original advisory:
http://www.microsoft.com/technet/security/Bulletin/MS06-010.mspx

Other references:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0004

CVE Reference: CVE-2006-0004

New Vulnerabilities found this Week

Windows Media Player Bitmap File Processing Vulnerability
"Remote code execution"

A remote code execution vulnerability exists in Windows Media Player because of the way that it handles processing bitmap files. An attacker could exploit the vulnerability by constructing a malicious bitmap file (.bmp) that could potentially allow remote code execution if a user visited a malicious Web site or viewed a malicious e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, significant user interaction is required to exploit this vulnerability.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-005.mspx
http://descriptions.securescout.com/tc/16124
http://www.eeye.com/html/research/advisories/AD20060214.html
http://www.kb.cert.org/vuls/id/291396

Windows Media Player Plug-in EMBED Element Buffer Overflow
"Remote code execution"

A remote code execution vulnerability exists in the Windows Media Player plug-in for non-Microsoft Internet browsers because of the way the Windows Media Player plug-in handles a malformed EMBED element. An attacker could exploit the vulnerability by constructing a malicious EMBED element that could potentially allow remote code execution if a user visited a malicious Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-006.mspx
http://descriptions.securescout.com/tc/16125
http://www.idefense.com/intelligence/vulnerabilities/display.php?id=393
http://www.kb.cert.org/vuls/id/692060

IBM Lotus Notes Multiple Vulnerabilities
"Stack-based buffer overflow; delete arbitrary files; execution of arbitrary code"

Secunia Research has discovered multiple vulnerabilities in Lotus Notes, which can be exploited by malicious people to bypass certain security restrictions or compromise a user's system.

1) A boundary error in kvarcve.dll when constructing the full pathname of a compressed file to check for its existence before extracting it from a ZIP archive can be exploited to cause a stack-based buffer overflow.

Successful exploitation allows execution of arbitrary code when the user extracts a compressed file with a long filename from within the Notes attachment viewer.

The vulnerability has been confirmed in version 6.5.4. Other versions may also be affected.

2) A boundary error in uudrdr.dll when handling UUE files containing an encoded file with an overly long filename can be exploited to cause a stack-based buffer overflow.

Successful exploitation allows execution of arbitrary code when a malicious UUE file is opened in the Notes attachment viewer.

The vulnerability has been confirmed in versions 6.5.4 and 7.0.

3) Directory traversal errors in kvarcve.dll when generating the preview of a compressed file from ZIP, UUE, and TAR archives can be exploited to delete arbitrary files that are accessible to the Notes user.

Successful exploitation requires that the user is e.g. tricked into previewing a compressed file with directory traversal sequences in its filename from within the Notes attachment viewer.

The vulnerability has been confirmed in versions 6.5.4 and 7.0. Prior versions may also be affected.

4) A boundary error in the TAR reader (tarrdr.dll) when extracting files from a TAR archive can be exploited to cause a stack-based buffer overflow via a TAR archive containing a file with a long filename.

Successful exploitation allows execution of arbitrary code, but requires that the user views a malicious TAR archive and chooses to extracts a compressed file to a directory with a very long path.

The vulnerability has been confirmed in versions 6.5.4 and 7.0. Prior versions may also be affected.

5) A boundary error exists in the HTML speed reader (htmsr.dll), which is used for viewing HTML attachments in emails. This can be exploited to cause a stack-based buffer overflow via a malicious email containing an overly long link beginning with either "http", "ftp", or "//".

Successful exploitation allows execution of arbitrary code with the privileges of the user running Lotus Notes, but requires that the user follows the link in the HTML document.

The vulnerability has been confirmed in versions 6.5.4 and 7.0. Prior versions may also be affected.

6) Another boundary error in the HTML speed reader when checking if a link references a local file can be exploited to cause a stack-based buffer overflow via a malicious email containing a specially crafted, overly long link.

Successful exploitation allows execution of arbitrary code with the privileges of the user running Lotus Notes, as soon as the user views the malicious HTML

document.

The vulnerability has been confirmed in versions 6.5.4 and 7.0. Prior versions may also be affected.

References:
http://www-1.ibm.com/support/docview.wss?rs=475&uid=swg21229918
http://www.kb.cert.org/vuls/id/884076

Mac OS X Kernel Local Denial of Service Vulnerability
"Denial of Service"

A vulnerability has been reported in Mac OS X, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

The vulnerability is caused due to an unspecified error in an undocumented system call. and can be exploited to crash the system.

References:
http://docs.info.apple.com/article.html?artnum=303290

Winamp File Handling Buffer Overflow Weaknesses
"Denial of Service"

Two weaknesses have been reported in Winamp, which can be exploited by malicious people to cause a DoS (Denial of Service).

1) A boundary error during the handling of files with an .m3u file extension can be exploited to cause a buffer overflow via a specially crafted playlist containing a file with an overly long filename.

2) A boundary error during the handling of overly long filenames can be exploited to cause a buffer overflow via a playlist containing a file with an overly long filename.

Successful exploitation crashes the application. Arbitrary code execution may be possible, but has not been proven.

The weaknesses have been reported in version 5.13. Other versions may also be affected.

References:
http://secway.org/advisory/AD20060216.txt

PostgreSQL Privilege Escalation and Denial of Service
"Denial of Service; gain escalated privileges"

Two vulnerabilities have been reported in PostgreSQL, which can be exploited by malicious users to cause a DoS (Denial of Service) or gain escalated privileges.

1) A validation error exists within the handling of the SET ROLE command when restoring the previous role setting after an error. This can be exploited by an authenticated user to gain superuser privileges.

The vulnerability has been reported in the 8.1 branch.

2) An error in the SET SESSION AUTHORIZATION command can be exploited to crash the server process, if it has been compiled with Asserts enabled.

The vulnerability has been reported in the 7.3, 7.4, 8.0 and 8.1 branch.

References:
http://archives.postgresql.org/pgsql-announce/2006-02/msg00008.php
http://www.postgresql.org/docs/8.1/static/release-7-3-14.html
http://www.postgresql.org/docs/8.1/static/release-7-4-12.html
http://www.postgresql.org/docs/8.1/static/release-8-0-7.html
http://www.postgresql.org/docs/8.1/static/release.html#RELEASE-8-1-3

Sun Solaris "in.rexecd" Privilege Escalation Vulnerability
"Gain escalated privileges"

A vulnerability has been reported in Sun Solaris, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to an unspecified error in the "in.rexecd" daemon. This can be exploited by malicious users to execute arbitrary commands with elevated privileges on Kerberos systems.

The vulnerability has been reported in Solaris 10 on both x86 and SPARC platforms.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102186-1

dotProject File Inclusion and Information Disclosure Vulnerabilities
"Disclose certain system information"

Robin Verton has discovered some vulnerabilities in dotProject, which can be exploited by malicious people to and compromise a vulnerable system.

1) Input passed to the "baseDir" parameter in "/includes/db_adodb.php", "/includes/db_connect.php", "/includes/session.php", "/modules/admin/vw_usr_roles.php", "/modules/public/calendar.php", and "/modules/public/date_format.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and

local resources.

Successful exploitation requires that "register_globals" is enabled.

2) Input passed to the "dPconfig[root_dir]" parameter in "/modules/projects/gantt.php", "/modules/projects/gantt2.php", "/modules/projects/vw_files.php", and "/modules/tasks/gantt.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources.

Successful exploitation requires that "register_globals" is enabled.

3) It is possible to disclose system configuration information by accessing "/docs/phpinfo.php" and "/docs/check.php".

The vulnerabilities have been confirmed in version 2.0.1. Other versions may also be affected.

Note: It is also possible to disclose path information when PHP "display_errors" is enabled by accessing files in the /db/ directory with certain parameters.

References:
http://secunia.com/advisories/18879/

GnuPG "gpgv" Signature Verification Security Issue
"Bypass certain security restrictions"

A security issue has been reported in GnuPG, which potentially can be exploited by malicious people to bypass certain security restrictions.

The security issue is caused due to "gpgv" exiting with a return code of 0 even if the detached signature file did not carry any signature. This may result in certain scripts that use "gpgv" to conclude that the signature is correctly verified.

Successful exploitation requires that "gpgv" or "gpg --verify" is used from a script that determines whether the file signature is correctly verified based on the return code.

The security issue has been reported in versions prior to 1.4.2.1.

References:
http://lists.gnupg.org/pipermail/gnupg-announce/2006q1/000211.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