netVigilance

ScoutNews Team

October 14, 2005
Issue # 41

Weekly ScoutNews by netVigilance

Table of Contents

Vote For SecureScout !

SC MAGAZINE AWARDS 2006

SC Magazine is holding their annual Best Products awards. Please take the time to put in a plug for your favorite Vulnerability Assessment tool; SecureScout NX. Follow the link below and enter your contact information.
Thank You !

Best Vulnerability Assessment –

SecureScout NX

This Week in Review

Exploit hits one day following patch Tuesday, more wireless security worries and Microsoft & open-source security?

Enjoy reading

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

Top Security News Stories this Week

❖ Windows exploit hits wild one day following vulnerability announcement

One day following the announcement by Microsoft of 14 new vulnerabilities. The exploit is against the MSDTC vulnerability within Windows, outlined in the Microsoft bulletin: MS05-051 security bulletin.

Windows 2000 systems are the target of this exploit; the most serious of the 14 disclosed Tuesday. W2K systems could fall victim to a Zotob type worm.
InformationWeek

Full Story:
http://www.informationweek.com/story/showArticle.jhtml?articleID=172300620

❖ ...Would you like data security with that?

Be careful when using those wireless access points that are commonly offered for fee or free at your local coffee boutique. Many of these popular hot spots cannot ensure the privacy of data while accessing them.

Attorneys for Starbucks have even issues a public warning regarding data security on their wireless networks; "These WLANs are not inherently secure," the company said. "We therefore cannot guarantee the privacy of your data and communications while using this service."
Scripps Howard News

Full Story :
http://www.shns.com/shns/g_index2.cfm?action=detail&pk=WIRELESS-VIRUS-10-13-05

❖ Microsoft driving open-source security?

Microsoft announced a couple of initiatives that it lauds as a cooperative effort to make it easier for security vendors to integrate and make the windows environment safer. First is the client protection solution template for security products. Secondly is the formation of the SecureIT Alliance; made up of major security software vendors.

Analyst Richard Williams of Garban Institutional Equities used terms like “Trojan Horse”, "straw dog" and "stalking horse" to describe the alliance.

Careful, that thing can bite! – *Ed.*

RedHerring

Full Story:
http://www.redherring.com/Article.aspx?a=13884&hed=Microsoft%e2%80%99s+Security+Alliance&sector=Industries&subsector=SecurityAndDefense

New Vulnerabilities Tested in SecureScout

❖ 14481 W32/Sober.r Worm (Registry Check)

This mass-mailing email virus arrives in an email message with one of the following attachment names:

KlassenFoto.zip
pword_change.zip
screen_photo.zip
privat-photo.zip
Inside the ZIP archive is a file named PW_Klass.Pic.packed-bitmap.exe or Screen_Photo.jpeg-graphic1.exe.

Like many Sober variants, this variant uses several different email messages randomly, in either English or German depending on the version of Windows.

The worm copies itself to a newly created directory in the WINDOWS directory and creates registry run keys to load itself at system startup.

The following files are created:

c:\WINDOWS\ConnectionStatus\netslot.nst
c:\WINDOWS\ConnectionStatus\services.exe
c:\WINDOWS\ConnectionStatus\socket.dli
It also drop these zero size files.

c:\WINDOWS\system32\bbvmwxxf.hml
c:\WINDOWS\system32\gdfjgthv.cvq
c:\WINDOWS\system32\langeinf.lin
c:\WINDOWS\system32\nonrunso.ber
c:\WINDOWS\system32\rubezahl.rub
c:\WINDOWS\system32\seppelmx.smx

** Further symptoms:

Desktop Firewalls displaying alerts due to the network activity of the worm:
Outgoing network traffic to port TCP 587
Outgoing network traffic to port TCP 37
Outgoing network traffic to port TCP 80 to the following domains:

people.freenet.de
home.arcor.de
home.pages.at
free.pages.at
scifi.pages.at

NOTE: The worm tries to download and execute files from these domains. The exact URL gets generated based on the current date and is likely to change during the next days and weeks, but the host address/domain will remain.

** Method of Infection

** Mail Propagation

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

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

References:

http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=136390

CVE Reference: GENERIC-MAP-NOMATCH

❖ 15698 Vulnerability in the Windows FTP Client Could Allow File Transfer Location Tampering (MS05-044/905495) (Remote File Checking)

A tampering vulnerability exists in the Windows FTP client. This vulnerability could allow an attacker to modify the intended destination location for a file transfer, when a client has manually chosen to transfer a file by using FTP. This vulnerability could allow the attacker to write the file to any file system that is located on an affected system.

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

References:

http://www.microsoft.com/technet/security/Bulletin/MS05-044.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2126

CVE Reference: CAN-2005-2126

❖ 15699 Vulnerability in Network Connection Manager Could Allow Denial of Service (MS05-045/905414) (Remote File Checking)

A denial of service vulnerability exists that could allow an attacker to send a specially crafted network packet to an affected system. An attacker who successfully exploited this vulnerability could cause the component responsible for managing network and remote access connections to stop responding. If the affected component is stopped due to an attack, it will automatically restart when new requests are received.

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

References:

http://www.microsoft.com/technet/security/Bulletin/MS05-045.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2307

CVE Reference: CAN-2005-2307

❖ 16016 Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution (MS05-046/899589) (Remote File Checking)

A remote code execution vulnerability exists in the Client Service for NetWare (CSNW) 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:

http://www.microsoft.com/technet/security/Bulletin/MS05-046.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1985

CVE Reference: CAN-2005-1985

❖ 16017 Vulnerability in Plug and Play Could Allow Remote Code Execution and Local Elevation of Privilege (MS05-047/905749) (Remote File Checking)

A remote code execution and local elevation of privilege vulnerability exists in Plug and Play that could allow an authenticated 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:

http://www.microsoft.com/technet/security/Bulletin/MS05-047.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2120

CVE Reference: CAN-2005-2120

❖ 16018 Vulnerability in the Microsoft Collaboration Data Objects Could Allow Remote Code Execution (MS05-048/907245) (Remote File Checking)

A remote code execution vulnerability exists in Collaboration Data Objects 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:

http://www.microsoft.com/technet/security/Bulletin/MS05-048.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1987

CVE Reference: CAN-2005-2120

❖ 16019 Vulnerabilities in Windows Shell Could Allow Remote Code Execution (MS05-049/900725) (Remote File Checking)

A remote code execution vulnerability exists in Windows because of the way that it handles the .lnk file name extension. By persuading a user to open an .lnk file that has specially-crafted properties an attacker could execute code on an affected system.

A remote code execution vulnerability exists in Windows because of the way that it handles files with the .lnk file name extension. By persuading a user to view the properties of a specially-crafted .lnk file, an attacker could execute code on the affected system.

A remote code execution vulnerability exists in the way that Web View in Windows Explorer handles certain HTML characters in preview fields. By persuading a user to preview a malicious file, an attacker could execute code. However, user interaction is required to exploit this vulnerability.

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

References:

http://www.microsoft.com/technet/security/Bulletin/MS05-049.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2122
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2118
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2117

CVE Reference: CAN-2005-2122, CAN-2005-2118, CAN-2005-2117

❖ 16020 Vulnerability in DirectShow Could Allow Remote Code Execution (MS5-050/904706) (Remote File Checking)

A remote code execution vulnerability exists in DirectShow 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:

http://www.microsoft.com/technet/security/Bulletin/MS05-050.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2128

CVE Reference: CAN-2005-2128

❖ 16021 Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution (MS05-051/902400) (Remote File Checking)

A remote code execution and local elevation of privilege vulnerability exists in the Microsoft Distributed Transaction Coordinator that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

A remote code execution and local elevation of privilege vulnerability exists in COM+ that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

A denial of service vulnerability exists that could allow an attacker to send a specially crafted network message to an affected system. An attacker could cause the Distributed Transaction Coordinator to stop responding.

A denial of service vulnerability exists that could allow an attacker to send a specially crafted network message to an affected system. An attacker could cause the Microsoft Distributed Transaction Coordinator (MSDTC) to stop responding. This specially crafted message could also be transferred through the affected system to another TIP server. This distributed attack could cause the MSDTC on both systems to stop responding.

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

References:

http://www.microsoft.com/technet/security/Bulletin/MS05-051.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2119
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1978
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1979
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1980

CVE Reference: CAN-2005-2119, CAN-2005-1978, CAN-2005-1979, CAN-2005-1980

❖ 16022 Cumulative Security Update for Internet Explorer (MS05-052/896688) (Remote File Checking)

A remote code execution vulnerability exists in the way Internet Explorer instantiates COM objects that are not intended to be instantiated in Internet Explorer. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited the 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:

http://www.microsoft.com/technet/security/Bulletin/MS05-052.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2127

CVE Reference: CAN-2005-2127

New Vulnerabilities found this Week

- **AVG Anti-Virus Engine Malformed ARJ Archive Virus Detection Bypass**

  "Bypass certain scanning functionality"

  fRoGGz has discovered a weakness in AVG Anti-Virus scan engine, which can be exploited by a malware to bypass certain scanning functionality.

  The weakness has been confirmed in AVG Email Server Edition version 7.0.344 (267.11.14/131) when scanning an email containing a malformed ".arj" archive with a NULL character prepended to the header. Other versions may also be affected.

  NOTE: This is not an issue on client systems, as the malware is still detected upon execution by the desktop on-access scanner.

  References:
  http://secunia.com/advisories/17126/

- **Clam AntiVirus OLE2 Unpacker Potential Denial of Service**

  "Denial of Service"

  Marcin Owsiany has discovered a vulnerability in Clam AntiVirus, which potentially can be exploited by malicious people to cause a DoS (Denial of Service).

  The vulnerability is caused due to an error in handling malformed OLE2 files (e.g. DOC files). This can be exploited to crash "clamd" via a specially crafted DOC file that causes "clamd" to call the "ole2_walk_property_tree()" function recursively.

  Successful exploitation causes a DoS (e.g. if "clamd" is used by an email gateway), but requires that "clamd" is configured with a large value (e.g. > 10000) for the ArchiveMaxFiles option.

  The vulnerability has been confirmed in version 0.87. Other versions may also be affected.

  References:
  http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=333566

- **Symantec Brightmail AntiSpam MIME Processing Denial of Service**

“Denial of Service”

A vulnerability has been reported in Brightmail AntiSpam, which potentially can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in processing certain malformed MIME content. This may be exploited to crash the "bmserver" component and cause a DoS.

The vulnerability has been reported in the following versions:
* Symantec Brightmail AntiSpam 6.0.1
* Symantec Brightmail AntiSpam 6.0.2

References:
http://securityresponse.symantec.com/avcenter/security/Content/2005.10.12d.html

- **Sun Java System Application Server JSP Source Code Disclosure**

“Disclose certain sensitive information”

A vulnerability has been reported in Sun Java System Application Server, which can be exploited by malicious people to disclose certain sensitive information.

The vulnerability is caused due to an unspecified error and can be exploited to disclose the source code of Java Server pages.

The vulnerability has been reported in the following versions on all platforms:
* Sun Java System Application Server 7 Standard Edition Update 6 and earlier
* Sun Java System Application Server 7 Platform Edition Update 6 and earlier
* Sun Java System Application Server 7 2004Q2 Standard Edition Update 2 and earlier
* Sun Java System Application Server 7 2004Q2 Enterprise Edition Update 2 and earlier

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101910-1

- **Linux Kernel Potential Denial of Service and Information Disclosure**

“Denial of Service”

Two vulnerabilities and a security issue have been reported in the Linux

Kernel, which potentially can be exploited by malicious, local users to cause a DoS (Denial of Service), or by malicious people to disclose certain sensitive information.

1) A memory leak in "/security/keys/request_key_auth.c" can potentially be exploited by non-privileged users to cause a DoS.

2) A memory leak exists in "/fs/namei.c" when the CONFIG_AUDITSYSCALL option is enabled. This can potentially be exploited by local users to cause a DoS via an excessive number of system calls.

3) The orinoco wireless driver fails to pad data packets with zeroes when the length needs to be increased. This may cause uninitialized data to be sent, potentially exposing random pieces of the system memory.

References:
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=74fd92c511bd4a0771ac0faaaef38bb1be3a29f6
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=829841146878e082613a49581ae252c071057c23
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=9bc39bec87ee3e35897fe27441e979e7c208f624
http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.14-rc4
http://o0o.nu/~meder/o0o_linux_orinoco_driver_info_leak.txt

❖ **WinRAR Format String and Buffer Overflow Vulnerabilities**
“Execute arbitrary code”

Secunia Research has discovered two vulnerabilities in WinRAR, which can be exploited by malicious people to compromise a user's system.

1) A format string error exists when displaying a diagnostic error message that informs the user of an invalid filename in an UUE/XXE encoded file. This can be exploited to execute arbitrary code when a malicious UUE/XXE file is decoded.

2) A boundary error in UNACEV2.DLL can be exploited to cause a stack-based buffer overflow. This allows arbitrary code execution when a malicious ACE archive containing a file with an overly long file name is extracted.

The vulnerabilities have been confirmed in version 3.50. Prior versions may also be affected.

References:
http://www.rarlabs.com/rarnew.htm
http://secunia.com/secunia_research/2005-53/advisory/

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