netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 19

May 12, 2006

Table of Contents

Product Focus

Sapphire Worm Scanner – scan up to 256 IP addresses for the existence of the Sapphire MS-SQL buffer overflow vulnerability.

This Week in Review

Malware is here to help you, Voting machines leave the back-door wide open, Oh really? a corny printer worm? and analysts are yawning over Vista security.

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

- **Trojan protects those that it infects?**

The Trojan/Erazer-A Trojan discovered this week, apparently seeks to protect the PCs that it infects. Engineers at Sophos that first discovered the Trojan, found that it deletes certain file types in specific download directories used by P2P programs. The assumption is that this piece of Malware is actually targeting common points of infection from P2P programs; deleting MP3, AVI, MPEG, WMV, Gif, Zip graphic and video files from specific locations.

Do not be deceived, this is still Malware. Who knows what havoc an “Erazer-B” or subsequent genus’s will wreak having gained the trust of naïve users.
TechWorld

Full Story :
http://www.techworld.com/security/news/index.cfm?newsID=6000&pagtype=all

❖ Diebold Voting machines contain ‘Dangerous’ vulnerability

Harri Hursti, a Finnish computer expert uncovered a very easily exploitable flaw in Diebold electronic voting machines whereby anyone with a little basic knowledge of Diebold voting systems and a standard component available at any computer store and a minute or two of access to a Diebold touch screen could load any software into the machine and gain complete control over it.

Elections officials in several states have asked that reports not contain detailed explanations because exploiting it is so simple and the tools for doing so are widely available.
[Maybe we should just resort to using slot machines; more secure with the same net effect – *Ed.*]
ChicoER.com

Full Story :
http://www.chicoer.com/news/bayarea/ci_3805089

❖ Comedic worm hits network printers

A new worm identified this week infects network printers, attempts to send a graphical image of an owl bearing the legend "O RLY?" to a number of print queues. Hoots-A worm is written in Visual Basic and spreads via network shares.

Although the Worm does not seem to cause any real damage, if does forebode more serious infections of a similar nature. [I do miss the days of the jokester-hackers – *Ed.*]
The Inquirer

Full Story :

http://www.theinquirer.net/?article=31671

❖ Vista ‘underwhelming’ on Security says Yankee

A report from Yankee Group Security Solutions & Services predicts that Vista OS security features will be more intrusive than helpful, causing users to disable them. Good new for some security vendors, Redmond won’t be dominating Sec. space anytime soon.
PCPro

Related Links :
http://www.pcpro.co.uk/security/news/87009/more-security-woes-for-vista.html

New Vulnerabilities Tested in SecureScout

❖ 16227 Ethereal SNDCP dissector, Denial of Service vulnerabilities (Remote File Checking)

Unspecified vulnerability in Ethereal 0.10.4 up to 0.10.14 allows remote attackers to cause a denial of service (abort) via the SNDCP dissector.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00023.html

Other references:
# DEBIAN:DSA-1049
# URL:http://www.debian.org/security/2006/dsa-1049
# FEDORA:FEDORA-2006-456
# URL:http://www.redhat.com/archives/fedora-announce-list/2006-April/msg00194.html
# FEDORA:FEDORA-2006-461
# URL:http://www.redhat.com/archives/fedora-announce-list/2006-April/msg00195.html
# GENTOO:GLSA-200604-17
# URL:http://www.gentoo.org/security/en/glsa/glsa-200604-17.xml
# MANDRIVA:MDKSA-2006:077
# URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:077
# BID:17682
# URL:http://www.securityfocus.com/bid/17682
# FRSIRT:ADV-2006-1501
# URL:http://www.frsirt.com/english/advisories/2006/1501
# SECTRACK:1015985

# URL:http://securitytracker.com/id?1015985
# SECUNIA:19769
# URL:http://secunia.com/advisories/19769
# SECUNIA:19805
# URL:http://secunia.com/advisories/19805
# SECUNIA:19828
# URL:http://secunia.com/advisories/19828
# SECUNIA:19839
# URL:http://secunia.com/advisories/19839

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

CVE Reference: CVE-2006-1940

❖ 16228 Ethereal telnet dissector, Buffer overflow vulnerability (Remote File Checking)

Buffer overflow in Ethereal 0.8.5 up to 0.10.14 allows remote attackers to execute arbitrary code via the telnet dissector.

The vulnerabilities have been reported in versions 0.8.5 up to 0.10.14.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00023.html

Other references:
# DEBIAN:DSA-1049
# URL:http://www.debian.org/security/2006/dsa-1049
# FEDORA:FEDORA-2006-456
# URL:http://www.redhat.com/archives/fedora-announce-list/2006-April/msg00194.html
# FEDORA:FEDORA-2006-461
# URL:http://www.redhat.com/archives/fedora-announce-list/2006-April/msg00195.html
# GENTOO:GLSA-200604-17
# URL:http://www.gentoo.org/security/en/glsa/glsa-200604-17.xml
# MANDRIVA:MDKSA-2006:077
# URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:077
# BID:17682
# URL:http://www.securityfocus.com/bid/17682
# FRSIRT:ADV-2006-1501
# URL:http://www.frsirt.com/english/advisories/2006/1501
# SECTRACK:1015985
# URL:http://securitytracker.com/id?1015985
# SECUNIA:19769
# URL:http://secunia.com/advisories/19769
# SECUNIA:19805
# URL:http://secunia.com/advisories/19805

# SECUNIA:19828
# URL:http://secunia.com/advisories/19828
# SECUNIA:19839
# URL:http://secunia.com/advisories/19839

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

CVE Reference: CVE-2006-1936

❖ 16229 Vulnerability in Microsoft Distributed Transaction Coordinator Could Allow Denial of Service (MS06-018/913580) (Remote File Checking)

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. Note that the denial of service vulnerability would not allow an attacker to execute code or to elevate their user rights, but it could cause the affected system to stop accepting requests.

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. Note that the denial of service vulnerability would not allow an attacker to execute code or to elevate their user rights, but it could cause the affected system to stop accepting requests.

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

References:

Original advisory:
* MS:MS06-018
* URL:http://www.microsoft.com/technet/security/bulletin/ms06-018.mspx

Other references:
* BUGTRAQ:20060509 [EEYEB20051011A] - Microsoft Distributed Transaction Coordinator Heap Overflow
* URL:http://www.securityfocus.com/archive/1/archive/1/433430/100/0/threaded
* MISC:http://www.eeye.com/html/research/advisories/AD20060509a.html
* BID:17906
* URL:http://www.securityfocus.com/bid/17906
* FRSIRT:ADV-2006-1742
* URL:http://www.frsirt.com/english/advisories/2006/1742
* SECUNIA:20000
* URL:http://secunia.com/advisories/20000
* BUGTRAQ:20060509 [EEYEB20051011B] - Microsoft Distributed Transaction Coordinator Denial of Service
* URL:http://www.securityfocus.com/archive/1/archive/1/433425/100/0/threaded
* MISC:http://www.eeye.com/html/research/advisories/AD20060509b.html
* BID:17905
* URL:http://www.securityfocus.com/bid/17905

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

CVE Reference: CVE-2006-1184, CVE-2006-0034

❖ 16230 Vulnerability in Microsoft Exchange Could Allow Remote Code Execution (MS06-019/916803) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Exchange Server that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

An attacker could exploit the vulnerability by constructing a specially crafted message that could potentially allow remote code execution when an Exchange Server processes an email with certain vCal or iCal properties.

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

References:

Original advisory:
* MS:MS06-019
* URL:http://www.microsoft.com/technet/security/bulletin/ms06-019.mspx

Other references:
* CERT:TA06-129A
* URL:http://www.us-cert.gov/cas/techalerts/TA06-129A.html
* CERT-VN:VU#303452
* URL:http://www.kb.cert.org/vuls/id/303452

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

CVE Reference: CVE-2006-0027

❖ 16232 Linux Kernel CIFS chroot Directory Traversal Vulnerability

Marcel Holtmann has reported a vulnerability in the Linux Kernel, which can be exploited by malicious, local users to bypass certain security restrictions.

The vulnerability is caused due to an input validation error in the CIFS mounted filesystem. This can be exploited to bypass chroot restrictions via the "..\\" directory traversal sequences.

The vulnerability has been reported in versions prior to 2.6.16.11.

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

References:

Original advisory:

https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=189434

Other references:
* CONFIRM:http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=296034f7de8bdf111984ce1630ac598a9c94a253
* TRUSTIX:2006-0024
* URL:http://www.trustix.org/errata/2006/0024
* BID:17742
* URL:http://www.securityfocus.com/bid/17742
* FRSIRT:ADV-2006-1542
* URL:http://www.frsirt.com/english/advisories/2006/1542
* OSVDB:25068
* URL:http://www.osvdb.org/25068
* SECUNIA:19868
* URL:http://secunia.com/advisories/19868

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-1863

❖ 16233 Linux Kernel SMBFS chroot Directory Traversal Vulnerability

Marcel Holtmann has reported a vulnerability in the Linux Kernel, which can be exploited by malicious, local users to bypass certain security restrictions.

The vulnerability is caused due to an input validation error in the SMBFS mounted filesystem. This can be exploited to bypass chroot restrictions via the "..\\" directory traversal sequences.

The vulnerability has been reported in versions prior to 2.6.16.14.

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

References:

Original advisory:
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=189435

Other references:
* BID:17735
* URL:http://www.securityfocus.com/bid/17735
* OSVDB:25067
* URL:http://www.osvdb.org/25067
* SECUNIA:19869
* URL:http://secunia.com/advisories/19869

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-1864

❖ 16234 Linux Kernel SCTP Netfilter Denial of Service Vulnerability

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

The vulnerability is caused due to missing checks on SCTP chunk sizes in the SCTP-netfilter code and may result in an infinite loop exhausting system resources.

The vulnerability has been reported in versions prior to 2.6.16.13.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.13

Other references:
* TRUSTIX:2006-0024
* URL:http://www.trustix.org/errata/2006/0024
* BID:17806
* URL:http://www.securityfocus.com/bid/17806
* FRSIRT:ADV-2006-1632
* URL:http://www.frsirt.com/english/advisories/2006/1632
* OSVDB:25229
* URL:http://www.osvdb.org/25229
* SECUNIA:19926
* URL:http://secunia.com/advisories/19926

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-1527

❖ 16235 Linux Kernel SCTP state table entries, kernel panic Vulnerability

The ECNE chunk handling in Linux SCTP (lksctp) before 2.6.16.15 allows remote attackers to cause a denial of service (kernel panic) via an unexpected chunk when the session is in CLOSED state.

The vulnerability has been reported in versions prior to 2.6.16.15.

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

References:

Original advisory:
http://git.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=35d63edb1c807bc5317e49592260e84637bc432e

Other references:
* FULLDISC:20060508 [MU-200605-01] Multiple vulnerabilities in Linux SCTP 2.6.16
* URL:http://archives.neohapsis.com/archives/fulldisclosure/2006-05/0227.html

* MISC:http://labs.musecurity.com/advisories/MU-200605-01.txt
* FRSIRT:ADV-2006-1734
* URL:http://www.frsirt.com/english/advisories/2006/1734
* SECUNIA:19990
* URL:http://secunia.com/advisories/19990

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-2271

❖ 16236 Linux Kernel fragmented SCTP COOKIE_ECHO and HEARTBEAT chunks, kernel panic Vulnerability

An error in the handling of incoming IP-fragmented SCTP control chunks can be exploited to cause kernel panic via fragmented COOKIE_ECHO and HEARTBEAT chunks.

The vulnerability has been reported in versions prior to 2.6.16.15.

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

References:

Original advisory:
http://labs.musecurity.com/advisories/MU-200605-01.txt

Other references:
* FULLDISC:20060508 [MU-200605-01] Multiple vulnerabilities in Linux SCTP 2.6.16
* URL:http://archives.neohapsis.com/archives/fulldisclosure/2006-05/0227.html
* CONFIRM:http://git.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=62b08083ec3dbfd7e533c8d230dd1d8191a6e813
* FRSIRT:ADV-2006-1734
* URL:http://www.frsirt.com/english/advisories/2006/1734
* SECUNIA:19990
* URL:http://secunia.com/advisories/19990

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-2272

❖ 16237 Linux Kernel SCTP message reassembly infinite recursion error

An infinite recursion error in the "sctp_skb_pull()" function of lksctp can be exploited to crash the system during message reassembly via a specially crafted packet that contains two or more DATA fragments of a message.

The vulnerability has been reported in versions prior to 2.6.16.15.

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

References:

Original advisory:
http://git.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=672e7cca17ed6036a1756ed34cf20dbd72d5e5f6

Other references:
http://secunia.com/advisories/19990/

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-2274

New Vulnerabilities found this Week

Microsoft Exchange Server Calendar Vulnerability
"Execution of arbitrary code"

A vulnerability has been reported in Microsoft Exchange Server, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an error within the EXCDO (Exchange Collaboration Data Objects) and CDOEX (Collaboration Data Objects for Exchange) functionality when processing iCal and vCal properties in email messages. This can be exploited by sending a specially crafted email message with certain vCal or iCal properties to a vulnerable server.

Successful exploitation allows execution of arbitrary code.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-019.mspx
http://descriptions.securescout.com/tc/16230

Linux Kernel "lease_init()" Denial of Service Vulnerability
"Denial of Service"

A vulnerability has been reported in the Linux Kernel, which potentially can be exploited by malicious, local users to cause a DoS (Denial of Service).

The vulnerability is caused due to a error within the "lease_init()" function in "fs/locks.c". This causes it to free memory that may not have been allocated using the "locks_alloc_lock()" function. This may cause the kernel to crash when the "fcntl_setlease()" function is called.

Note: A slab leak in "__setlease()" due to an uninitialised return value has also been reported.

References:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.16

Microsoft Windows "itss.dll" Heap Corruption Vulnerability

“Boundary error”

Rubén Santamarta has discovered a vulnerability in Microsoft Windows, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the Infotech Storage System Library (itss.dll) when reading a ".CHM" file. This can be exploited to cause heap corruption and may allow arbitrary code execution via a specially crafted ".CHM" file.

Successful exploitation requires that the user is e.g. tricked in opening or decompiling a malicious ".CHM" file using "hh.exe".

The vulnerability has been confirmed in Windows XP SP2 (fully patched) and also reported in Windows 2000 SP4. Other versions may also be affected.

NOTE: The CHM file format should be considered insecure and treated similar to an executable file. However, this vulnerability is triggered even when the user decompiles the file without opening it.

References:
http://reversemode.com/index.php?option=com_content&task=view&id=11&Itemid=1

Microsoft Distributed Transaction Coordinator Two Vulnerabilities
“Denial of Service”

Two vulnerabilities have been reported in Microsoft Windows, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

1) An out-of-bounds memory access error in the MSDTC (Microsoft Distributed Transaction Coordinator) can be exploited via a specially crafted BuildContextW request with a large UuidString or GuidIn string.

Successful exploitation causes the MSDTC component and dependent services to stop responding.

2) A boundary error in the "CRpcIoManagerServer::BuildContext()" function in msdtcprx.dll within MSDTC can be exploited to cause a heap-based buffer overflow. According to the vendor, this causes the MSDTC component and dependent services to stop responding when receiving a specially crafted network message.

According to eEye Digital Security, this vulnerability can be exploited to execute arbitrary code on a vulnerable system.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-018.mspx
http://descriptions.securescout.com/tc/16229

Linux Kernel SCTP Denial of Service Vulnerabilities
“Denial of Service”

Some vulnerabilities have been reported in the Linux Kernel, which can be exploited by malicious people to cause a DoS (Denial of Service).

1) An incorrect use of state table entries in the SCTP code when certain ECNE chunks are received in CLOSED state can be exploited to cause kernel panic via a specially crafted packet.

2) An error in the handling of incoming IP-fragmented SCTP control chunks can be exploited to cause kernel panic via fragmented COOKIE_ECHO and HEARTBEAT chunks.

3) An infinite recursion error in the "sctp_skb_pull()" function of lksctp can be exploited to crash the system during message reassembly via a specially crafted packet that contains two or more DATA fragments of a message.

4) An deadlock error within the handling of the receive buffer in SCTP can be exploited to cause a DoS via a large number of small messages sent to a receiver application that causes it to run of receive buffer space.

The vulnerabilities have been reported in version 2.6.16. Other versions may also be affected.

References:
http://labs.musecurity.com/advisories/MU-200605-01.txt

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