netVigilance

ScoutNews Team

March 17, 2006
2006 Issue # 11

Weekly ScoutNews by netVigilance

Table of Contents

New in SecureScout

Product Spotlight: Messenger Service Vulnerability Scanner – This free SecureScout single scanner checks up to 256 IP addresses for the Microsoft Windows Messenger Service flaw (MS03-043).

This Week in Review

McAfee DAT file kills hundreds of harmless applications, Hackers resorting to sneaky targeted attacks, eBay / Chase attacks traced back to State-Owned Chinese bank and nasty DDoS attack discovered in the wild.

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

- **McAfee update kills numerous applications**

McAfee's on-demand-scanning products erroneously marked hundreds of application files as the 2004 Virus W95/CTX. The affected application files included numerous types from Microsoft, Adobe, Sun Microsystems JAVA, Adaptec, Google and others.

Depending on how a user had McAfee configured, the files could have been deleted.

TechWeb

Full Story :
http://www.techweb.com/wire/security/181503287;jsessionid=PLVODSRICW34CQSNDBECKH0CJUMEKJVN

- **Targeted attacks becoming more popular**

In order to circumvent anti-virus and intrusion prevention technology; hackers are turning away from broad-based attacks and resorting to isolated, directed methods.

These new attacks come in the form of spear-phishing or quietly infecting say a Word document and spreading slowly once inside an organization.

These types of attacks go largely undetected and do not get the attention of the major anti-virus companies. Virus' in the past flood the internet, infecting millions of computers very quickly. The Honeypots at Anti-virus companies get infected too and signatures are developed to thwart the infection.

Spear-phishing targets say a single department within a corporation, the virus infects for instance; a Word documents then spreads quietly through copies of these files. Hackers will be able to fly under the radar for a long time.

TechRepublic

Full Story :
http://techrepublic.com.com/5100-1009_11-6049117.html#

- **eBay, Chase phishing scam traced to Chinese bank**

Phishers posing as representatives from eBay and Chase Manhattan Bank were traced back to sites hosted on IP addresses belonging to the Shanghai Branch of The China Construction Bank (CCB).

The British security firm Netcraft discovered the first ever incidence of the infrastructure of one financial institution being used to attack another. Duped users were asked for their username and password in order to deposit a $20 "reward."

Yahoo

Full Story :

http://news.yahoo.com/s/afp/20060314/tc_afp/usitinternetfraudchina

- **Verisign raises alarm on pending DDoS attacks**

On Thursday, VeriSign issued a warning about the emergence of a very intense Distributed Denial of Service (DDoS) attack. This new type of attack is disturbing in the way that it takes advantage of mis-configured DNS servers to reflect the attack onto a target. The resulting DoS attack on the target can run into the multi-Gigabit range.
ComputerWorld

Full Story :
http://www.networkworld.com/news/2006/031606-denial-of-service-attacks.html?fsrc=netflash-rss

New Vulnerabilities Tested in SecureScout

- **16159 Permissive Windows Services DACLs Could Allow Elevation of Privilege (MS06-011/914798) (Registry Check)**

A privilege elevation vulnerability exists on Windows XP Service Pack 1 on the identified Windows services where the permissions are set by default to a level that may allow a low-privileged user to change properties associated with the service. On Windows 2003 permissions on the identified services are set to a level that may allow a user that belongs to the network configuration operators group to change properties associated with the service. Only members of the Network Configuration Operators group on the targeted machine can remotely attack Windows Server 2003, and this group contains no users by default. The vulnerability could allow a user with valid logon credentials to take complete control of the system on Microsoft Windows XP Service Pack 1.

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

References:

Original advisory:
* MS:MS06-011
* URL:http://www.microsoft.com/technet/security/bulletin/ms06-011.mspx

Other references:
* BUGTRAQ:20060131 Windows Access Control Demystified
* URL:http://www.securityfocus.com/archive/1/archive/1/423587/100/0/threaded
* MISC:http://www.cs.princeton.edu/~sudhakar/papers/winval.pdf
* MISC:http://www.microsoft.com/technet/security/advisory/914457.mspx
* CERT-VN:VU#953860
* URL:http://www.kb.cert.org/vuls/id/953860

* FRSIRT:ADV-2006-0417
* URL:http://www.frsirt.com/english/advisories/2006/0417
* SECTRACK:1015595
* URL:http://securitytracker.com/id?1015595
* SECTRACK:1015765
* URL:http://securitytracker.com/id?1015765
* SECUNIA:18756
* URL:http://secunia.com/advisories/18756
* XF:win-auth-users-insecure-permissions(24463)
* URL:http://xforce.iss.net/xforce/xfdb/24463

CVE Reference: CVE-2006-0023

❖ 16160 Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (MS06-012/905413) (Remote File Checking)

A remote code execution vulnerability exists in Excel using a malformed range. An attacker could exploit the vulnerability by constructing a specially crafted Excel file that could allow remote code execution.

If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

A remote code execution vulnerability exists in Excel using a malformed parsing format file. An attacker could exploit the vulnerability by constructing a specially crafted Excel file that could allow remote code execution.

If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

A remote code execution vulnerability exists in Excel using a malformed description. An attacker could exploit the vulnerability by constructing a specially crafted Excel file that could allow remote code execution.

If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

A remote code execution vulnerability exists in Excel using malformed graphic. An attacker could exploit the vulnerability by constructing a specially crafted Excel file that could allow remote code execution.

If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

A remote code execution vulnerability exists in Excel using a malformed record. An attacker could exploit the vulnerability by constructing a specially crafted Excel file that could allow remote code execution.

If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

A remote code execution vulnerability exists in Office. An attacker could exploit the vulnerability by constructing a specially crafted routing slip within an Office document that could allow remote code execution. An attacker who successfully exploited this vulnerability could take complete control of the affected system.

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

References:

Original advisory:
MS:MS06-012
URL:http://www.microsoft.com/technet/security/bulletin/ms06-012.mspx

Other references:
MISC:http://www.eweek.com/article2/0,1759,1899697,00.asp?kc=EWRSS03129TX1K0000614
MISC:http://news.zdnet.com/2100-1009_22-5989078.html
MISC:http://informationweek.com/story/showArticle.jhtml?articleID=174910198
MISC:http://www.theage.com.au/news/breaking/excel-flaw-up-for-sale-on-ebay/2005/12/09/1134086783318.html
MISC:http://www.securityfocus.com/news/11363
MISC:http://news.com.com/2061-10789_3-5988086.html
MISC:http://www.theregister.co.uk/2005/12/10/ebay_pulls_excel_vulnerability_auction/
MISC:http://www.osvdb.org/blog/?p=71
BUGTRAQ:20060314 High Risk Vulnerability in Microsoft Excel
URL:http://www.securityfocus.com/archive/1/archive/1/427635/100/0/threaded
BUGTRAQ:20060315 [HV-HIGH] Microsoft Excel Named Range Arbitrary Code Execution
URL:http://www.securityfocus.com/archive/1/archive/1/427698/100/0/threaded
CERT:TA06-073A
URL:http://www.us-cert.gov/cas/techalerts/TA06-073A.html
CERT-VN:VU#642428
URL:http://www.kb.cert.org/vuls/id/642428
BID:15780
URL:http://www.securityfocus.com/bid/15780
SECTRACK:1015333

URL:http://securitytracker.com/id?1015333
SECTRACK:1015766
URL:http://securitytracker.com/id?1015766
SECUNIA:19138
URL:http://secunia.com/advisories/19138
XF:excel-msvcrt-memmove-bo(23537)
URL:http://xforce.iss.net/xforce/xfdb/23537
BUGTRAQ:20060314 ZDI-06-004: Microsoft Excel File Format Parsing Vulnerability
URL:http://www.securityfocus.com/archive/1/archive/1/427632/100/0/threaded
CERT-VN:VU#339878
URL:http://www.kb.cert.org/vuls/id/339878
XF:excel-parsing-format-file-bo(25225)
URL:http://xforce.iss.net/xforce/xfdb/25225
CERT-VN:VU#235774
URL:http://www.kb.cert.org/vuls/id/235774
XF:excel-description-bo(25227)
URL:http://xforce.iss.net/xforce/xfdb/25227
CERT-VN:VU#123222
URL:http://www.kb.cert.org/vuls/id/123222
OSVDB:23901
URL:http://www.osvdb.org/23901
VULNWATCH:20060315 [xfocus-SD-060314]Microsoft Office Excel Buffer Overflow Vulnerability
CERT-VN:VU#104302
URL:http://www.kb.cert.org/vuls/id/104302
BID:17101
URL:http://www.securityfocus.com/bid/17101
XF:excel-record-bo(25228)
URL:http://xforce.iss.net/xforce/xfdb/25228
BUGTRAQ:20060314 SYMSA-2006-001: Buffer overflow in Microsoft Office 2000, Office XP (2002), and Office 2003 Routing Slip Metadata
URL:http://www.securityfocus.com/archive/1/archive/1/427671/100/0/threaded
CERT-VN:VU#682820
URL:http://www.kb.cert.org/vuls/id/682820
BID:17000
URL:http://www.securityfocus.com/bid/17000

CVE Reference: CVE-2005-4131, CVE-2006-0028, CVE-2006-0029, CVE-2006-0030, CVE-2006-0031, CVE-2006-0009

❖ 16162 Linux Kernel information leak in the "ext2_make_empty()" function to disclose kernel memory

A vulnerability has been reported in the Linux kernel, which can be exploited to disclose kernel memory.

An information leak exists in the "ext2_make_empty()" function in the implementation of the ext2 filesystem when creating new directories. This can be exploited to disclose kernel memory.

The vulnerability has been reported in versions 2.4. through 2.4.30-rc2 and 2.6 through 2.6.11.6

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

Attack

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.12-rc1

Other references:
* BUGTRAQ:20050401 Information leak in the Linux kernel ext2 implementation
* URL:http://marc.theaimsgroup.com/?l=bugtraq&m=111238764720696&w=2
* MISC:http://arkoon.net/advisories/ext2-make-empty-leak.txt
* FEDORA:FLSA:152532
* URL:https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=152532
* REDHAT:RHSA-2006:0190
* URL:http://www.redhat.com/support/errata/RHSA-2006-0190.html
* REDHAT:RHSA-2006:0191
* URL:http://www.redhat.com/support/errata/RHSA-2006-0191.html
* UBUNTU:USN-103-1
* URL:http://www.ubuntulinux.org/support/documentation/usn/usn-103-1
* SECUNIA:18684
* URL:http://secunia.com/advisories/18684
* XF:kernel-ext2-information-disclosure(19866)
* URL:http://xforce.iss.net/xforce/xfdb/19866
* CONFIRM:http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11.6
* SECUNIA:14713
* URL:http://secunia.com/advisories/14713/

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-0400

❖ 16163 Linux Kernel error in load_elf_library to cause a Denial of Service

A vulnerability has been reported in the Linux kernel, which can be exploited to cause a DoS.

An error in load_elf_library can be exploited to cause a DoS.

The vulnerability has been reported in versions 2.4. through 2.4.30-rc2 and 2.6 through 2.6.11.6

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.12-rc1

Other references:
* FEDORA:FLSA:152532
* URL:https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=152532
* UBUNTU:USN-103-1
* URL:http://www.ubuntulinux.org/support/documentation/usn/usn-103-1

* CONFIRM:http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11.6
* SECUNIA:14713
* URL:http://secunia.com/advisories/14713/
* XF:kernel-loadelflibrary-dos(19867)
* URL:http://xforce.iss.net/xforce/xfdb/19867

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-0749

❖ 16164 Linux Kernel error in the "fib_seq_start()" function to crash the system

A vulnerability has been reported in the Linux kernel, which can be exploited to crash the system.

An error in the "fib_seq_start()" function can be exploited by malicious, local users to crash the system via /proc/net/route.

The vulnerability has been reported in versions 2.4. through 2.4.30-rc2 and 2.6 through 2.6.11.6

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.12-rc1

Other references:
* MLIST:[bk-commits-head] 20050319 [PATCH] Fix crash while reading /proc/net/route
* URL:http://marc.theaimsgroup.com/?l=bk-commits-head&m=111186506706769&w=2
* SUSE:SUSE-SA:2005:068
* URL:http://www.securityfocus.com/archive/1/archive/1/419522/100/0/threaded
* BID:13267
* URL:http://www.securityfocus.com/bid/13267
* SECUNIA:17918
* URL:http://secunia.com/advisories/17918

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-1041

❖ 16165 Linux Kernel boundary error in the "rose_rt_ioctl()" function to be exploited to crash the kernel

A vulnerability has been reported in the Linux kernel and can be exploited to crash the kernel.

A boundary error exists in the ROSE "rose_rt_ioctl()" function due to missing verification

of the ndigis argument of new routes. This can be exploited to crash the kernel by calling the function with a large ngidis argument.

The vulnerability has been reported in versions 2.6 through 2.6.12-rc1 not included.

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

References:

Original advisory:
http://lkml.org/lkml/2005/5/23/169

Other references:
* CONFIRM:http://linux.bkbits.net:8080/linux-2.4/cset@41e2cf515TpixcVQ8q8HvQvCv9E6zA
* CONFIRM:http://linux.bkbits.net:8080/linux-2.6/cset@423114bcdthRtmtdS6MsZiBVvteGCg
* DEBIAN:DSA-922
* URL:http://www.debian.org/security/2005/dsa-922
* MANDRAKE:MDKSA-2005:218
* URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:218
* MANDRAKE:MDKSA-2005:219
* URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:219
* MANDRAKE:MDKSA-2005:220
* URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:220
* MANDRIVA:MDKSA-2005:219
* URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:219
* MANDRIVA:MDKSA-2005:220
* URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:220
* UBUNTU:USN-219-1
* URL:http://www.ubuntulinux.org/support/documentation/usn/usn-219-1
* BID:13886
* URL:http://www.securityfocus.com/bid/13886
* SECTRACK:1014115
* URL:http://securitytracker.com/id?1014115
* SECUNIA:18056
* URL:http://secunia.com/advisories/18056

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-3273

❖ 16166 Linux Kernel user with permissions to access a SCSI tape device can cause it to become unusable

A vulnerability has been reported in the Linux kernel and can be exploited to deny access to a SCSI tape device.

Any user with permissions to access a SCSI tape device can send some commands, which may cause it to become unusable for other users.

The vulnerability has been reported in versions 2.6 through 2.6.12-rc1 not included.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.12-rc1
http://kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.12-rc2

Other references:
http://secunia.com/advisories/14585/

Product HomePage:
http://kernel.org/

CVE Reference: None

❖ 16167 Linux Kernel race condition in ebtables netfilter module (ebtables.c) to cause a DoS (kernel panic)

A vulnerability has been reported in the Linux kernel and can be exploited to cause a DoS (kernel panic).

A race condition in ebtables netfilter module (ebtables.c) when running on an SMP system operating under a heavy load, may be exploited to cause a DoS (kernel panic) via a series of packets.

The vulnerability has been reported in versions 2.6 through 2.6.12-rc1 not included.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.12-rc1
http://kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.12-rc2

Other references:
*
CONFIRM:http://sourceforge.net/mailarchive/forum.php?thread_id=6800453&forum_id=8572
* DEBIAN:DSA-922
* URL:http://www.debian.org/security/2005/dsa-922
* REDHAT:RHSA-2005:808
* URL:http://www.redhat.com/support/errata/RHSA-2005-808.html
* SUSE:SUSE-SA:2005:068
* URL:http://www.securityfocus.com/archive/1/archive/1/419522/100/0/threaded
* UBUNTU:USN-199-1
* URL:http://www.ubuntu.com/usn/usn-199-1
* BID:15049
* URL:http://www.securityfocus.com/bid/15049
* SECUNIA:17364
* URL:http://secunia.com/advisories/17364

* SECUNIA:17918
* URL:http://secunia.com/advisories/17918
* SECUNIA:18056
* URL:http://secunia.com/advisories/18056

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-3110

❖ 16168 Linux Kernel error in the maintaining of cache coherency to be exploited to cause a DoS and possibly corrupt data

A vulnerability has been reported in the Linux kernel and can be exploited to cause a DoS and possibly corrupt data by modifying PTE protections.

An error in the maintaining of cache coherency in "mprotect.c" on Itanium IA64 processors can be exploited by local users to cause a DoS and possibly corrupt data by modifying PTE protections.

The vulnerability has been reported in versions 2.6 through 2.6.12-rc1 not included.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.12-rc1
http://kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.12-rc2

Other references:
* MISC:http://www.intel.com/cd/ids/developer/asmo-na/eng/215766.htm
* MISC:http://cache-www.intel.com/cd/00/00/21/57/215792_215792.pdf
* CONFIRM:http://linux.bkbits.net:8080/linux-2.6/cset@4248d4019z8HvgrPAji51TKrWiV2uw?nav=index.html|src/|src/mm|related/mm/mprotect.c
* DEBIAN:DSA-922
* URL:http://www.debian.org/security/2005/dsa-922
* SECUNIA:18056
* URL:http://secunia.com/advisories/18056

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-3105

❖ 16169 Linux Kernel PPP Server Denial of Service

Ben Martel and Stephen Blackheath have reported a vulnerability in the Linux kernel, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error within the LCP (Link Control Protocol)

parsing in the "ppp_async.c" driver and can be exploited by pppd clients to cause the server to hang.

The vulnerability has been reported in versions 2.6 through 2.6.11.4 not included.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11.4

Other references:
* FEDORA:FLSA:152532
* URL:https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=152532
* REDHAT:RHSA-2005:283
* URL:http://www.redhat.com/support/errata/RHSA-2005-283.html
* REDHAT:RHSA-2005:284
* URL:http://www.redhat.com/support/errata/RHSA-2005-284.html
* SUSE:SUSE-SA:2005:018
* URL:http://www.novell.com/linux/security/advisories/2005_18_kernel.html
* TRUSTIX:2005-0009
* URL:http://www.trustix.org/errata/2005/0009/
* UBUNTU:USN-95-1
* URL:http://www.ubuntulinux.org/support/documentation/usn/usn-95-1

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-0384

New Vulnerabilities found this Week

Microsoft Office Multiple Code Execution Vulnerabilities
"Execution of arbitrary code"

Multiple vulnerabilities have been reported in Microsoft Office, which can be exploited by malicious people to compromise a user's system.

1) A boundary error in Excel when processing files with a malformed "Named Range" with negative length values can be exploited to corrupt memory and allows execution of arbitrary code on a user's system when viewing a specially crafted Excel file.

2) A boundary error in Office when processing documents containing a specially crafted "routing slip" can be exploited to corrupt memory and allows execution of arbitrary code on a user's system when the user views and closes a malicious document.

3) An error in Excel when parsing the BIFF file format can be exploited via malformed BOOLERR records to corrupt memory. This allows execution of arbitrary code on a user's system when viewing a specially crafted Excel file.

4) A boundary error in Excel when processing a specially crafted file with an overly large formula size can be exploited to cause a stack-based buffer overflow and allows execution of arbitrary code on a user's system when a malicious Excel file is viewed. An error within the handling of the "Column Index" read from an Excel file can cause Excel to crash due to invalid memory access.

5) An error in Excel when processing malformed graphics can be exploited to corrupt memory and allows execution of arbitrary code on a user's system when viewing a specially crafted Excel file.

6) A boundary error in Excel when processing malformed records with a specially-crafted length value can be exploited to corrupt stack memory and may allow execution of arbitrary code on a user's system when viewing a malicious Excel file.

References:
http://descriptions.securescout.com/tc/16160
http://www.microsoft.com/technet/security/Bulletin/MS06-012.mspx
http://www.kb.cert.org/vuls/id/104302
http://www.kb.cert.org/vuls/id/123222
http://www.kb.cert.org/vuls/id/235774
http://www.kb.cert.org/vuls/id/339878
http://www.kb.cert.org/vuls/id/642428
http://www.kb.cert.org/vuls/id/682820

OpenOffice cURL/libcURL URL Parsing Off-By-One Vulnerability

A vulnerability has been reported in OpenOffice, which has an unknown impact.

The vulnerability is caused due to the use of a vulnerable version of cURL/libcURL.

The vulnerability has been reported in versions prior to 2.0.2.

References:
http://qa.openoffice.org/issues/show_bug.cgi?id=59032

Apache Log4net Denial of Service Vulnerability
"Denial of Service"

Sebastian Krahmer has reported a vulnerability in Log4net, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an unspecified error in LocalSyslogAppender. This can be exploited to cause memory corruption in an application that uses LocalSyslogAppender and may cause the application to crash.

The vulnerability has been reported in version 1.2.9. Prior versions may also be affected.

References:
http://issues.apache.org/jira/browse/LOG4NET-67

Apache mod_python FileSession Handling Vulnerability

"Gain escalated privileges"

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

The vulnerability is caused due to a directory traversal error when FileSession is used to keep sessions in mod_python. This can potentially be exploited by a logon user, or by a user who can write to the filesystem, to execute arbitrary code with privileges of the web server.

The vulnerability has been reported in version 3.2.7.

References:
http://www.modpython.org/fs_sec_warn.html
http://svn.apache.org/viewcvs.cgi/httpd/mod_python/branches/3.2.x/NEWS?rev=378945

Mac OS X Security Update Fixes Multiple Vulnerabilities
"Buffer overflow; malicious file to be executed automatically"

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

1) Under certain circumstances, it is possible for JavaScript to bypass the same-origin policy via specially crafted archives.

2) A boundary error in Mail can be exploited to cause a buffer overflow via a specially crafted email with an overly long Real Name entry. This allows execution of arbitrary code on a user's system if a specially crafted attachment in the AppleDouble format is double-clicked.

3) An error in Safari / LaunchServices can cause a malicious application to appear as a safe file type. This may cause a malicious file to be executed automatically when visiting a malicious web site.

References:
http://docs.info.apple.com/article.html?artnum=303453

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