netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 26

July 6, 2007

Table of Contents

Product Focus

Spida Digispid Worm Scanner – The Spida Digispid Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are prone any of the Microsoft Java Virtual Machine Vulnerabilities (MS02-069). machines.

This Week in Review

New internet portal for security research. Huge increase in web based malware.Beijing world virus capital.Internet terrorist conviction.

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

- **Finally A Marketplace Site For Security Research**

Switzerland, 4th July 2007 - A revolution in the way security research is handled and reported has occurred!...

WSLabi (www.wslabi.com), a neutral vendor independent Swiss laboratory, has launched a new international security research exchange. This exchange will create a portal where researchers, security vendors and software companies can interact in an open market to enable researcher's to obtain the correct value for their findings. The exchange will become a global database of every IT security research ever found.

According to Herman Zampariolo, CEO of WSLabi, "We decided to set up this portal for selling security research because although there are many researchers out there who discover vulnerabilities very few of them are able or willing to report it to the 'right' people due to the fear of being exploited.

ITBackbones

Full Story :
http://www.itbsecurity.com/pr/15058

❖ Nearly 30,000 Malicious Web Sites Appear Each Day

While researchers are simply getting better at finding the malicious sites, Sophos reports that hackers are increasingly turning to Web-borne malware -- in great numbers.
The number of malicious Web sites has skyrocketed over the past few months, going from 5,000 new ones a day in April to nearly 30,000 a day now.

"This certainly is a huge increase," said Carole Theriault, a senior security consultant with Sophos, in an e-mail to InformationWeek. "In June, we saw it climb to 9,500 a day and then this huge jump up 29,000."

Theriault said there is a two-pronged reason for the remarkable increase.

One reason is that hackers are increasingly turning away from e-mail as their preferred method of spreading malware and putting their focus on the malicious Web site. In some cases, they're creating their own malicious Web sites, but in most cases they're hacking into legitimate sites and embedding malware into them.
informationweek

Full Story :
http://www.informationweek.com/research/showArticle.jhtml?articleID=200001941&cid=RSSfeed_TechWeb

❖ Beijing accused of being world virus capital

The Chinese capital city Beijing tops the global league table for distributing viruses, a new survey has reported.
According to UK-based managed security services companyNetwork Box, Beijing accounts for 40 percent of all viruses that passed though the company's servers in June, and 5.25 percent of detected spam.

This compares with slightly lower percentages for cities in countries noted for having a malware problem. Moscow was second for spam with 5.12 percent, Seoul third with 3.58

percent, Turk in Turkey fourth with 3.4 percent, and London in fifth place on 2.47 percent, statistics that are likely to be skewed to some extent by the company's UK-based customer base.

computerworlduk

Full Story :
http://www.computerworlduk.com/management/security/cybercrime/news/index.cfm?RSS&NewsId=3867

- **First ever UK conviction for internet terrorism**

Three men said to be linked to al-Qaeda, including one using an Arabic name meaning "Terrorist 007", have admitted inciting terrorism over the internet in the first case of its kind in Britain, police said on Wednesday.

The men, said by prosecutors to have close ties to Osama Bin Laden's network, pleaded guilty to inciting acts of terrorism "wholly or partly" outside Britain via websites which advocated the killing of non-Muslims.

Moroccan-born Younes Tsouli, Briton Waseem Mughal and Jordanian-born Tariq Al-Daour changed their original "not guilty" pleas part way through a trial which had begun at Woolwich Crown Court in east London in April.

zdnet

Full Story :
http://news.zdnet.co.uk/itmanagement/0,1000000308,39287873,00.htm

New Vulnerabilities Tested in SecureScout

- **16546 Linux Kernel netlink NETLINK_FIB_LOOKUP Denial of Service**

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

The vulnerability is caused due to an error within the handling of NETLINK_FIB_LOOKUP reply messages. This can be exploited to cause an infinite recursion, which could result in a stack overflow.

The vulnerability is reported in versions prior to 2.6.20.8. Other versions may also be affected.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.20.8

Other references:
BUGTRAQ:20070615 rPSA-2007-0124-1 kernel xen
URL:http://www.securityfocus.com/archive/1/471457
CONFIRM: https://issues.rpath.com/browse/RPL-1309
CONFIRM: https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=237913
DEBIAN:DSA-1289
URL:http://www.debian.org/security/2007/dsa-1289
REDHAT:RHSA-2007:0347
URL:http://www.redhat.com/support/errata/RHSA-2007-0347.html
BID:23677
URL:http://www.securityfocus.com/bid/23677
FRSIRT:ADV-2007-1595
URL:http://www.frsirt.com/english/advisories/2007/1595
SECUNIA:25030
URL:http://secunia.com/advisories/25030
SECUNIA:25083
URL:http://secunia.com/advisories/25083
SECUNIA:25228
URL:http://secunia.com/advisories/25228
SECUNIA:25288
URL:http://secunia.com/advisories/25288
SECUNIA:25691
URL:http://secunia.com/advisories/25691

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2007-1861

❖ 16545 Linux Kernel RTA_MAX Denial of Service Vulnerability

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

A boundary error due to the use of RTA_MAX instead of RTN_MAX in dn_fib_props[] within dn_fib.c and in fib_props[] within fib_semantics.c can potentially be exploited to cause a DoS.

The vulnerability is reported in versions prior to 2.6.21.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.21-rc6

Other references:
CONFIRM: http://www.mail-archive.com/git-commits-head@vger.kernel.org/msg08269.html
CONFIRM: http://www.mail-archive.com/git-commits-head@vger.kernel.org/msg08270.html
REDHAT:RHSA-2007:0347
URL:http://www.redhat.com/support/errata/RHSA-2007-0347.html
REDHAT:RHSA-2007:0488
URL:http://rhn.redhat.com/errata/RHSA-2007-0488.html
UBUNTU:USN-464-1
URL:http://www.ubuntu.com/usn/usn-464-1
BID:23447
URL:http://www.securityfocus.com/bid/23447
SECUNIA:25288
URL:http://secunia.com/advisories/25288
SECUNIA:25392
URL:http://secunia.com/advisories/25392

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2007-2172

❖ 16544 Linux Kernel IPv6 Type 0 Route Headers Denial of Service Vulnerability

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

An error exists within the processing of packets with IPv6 type 0 route headers. This can be exploited to cause a DoS due to high network traffic by sending specially crafted IPv6 packets to vulnerable systems.

The vulnerability is reported in versions prior to 2.6.21..

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.21

Other references:
BUGTRAQ:20070615 rPSA-2007-0124-1 kernel xen
URL:http://www.securityfocus.com/archive/1/471457
MISC: http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf
CONFIRM: https://issues.rpath.com/browse/RPL-1310
FREEBSD:FreeBSD-SA-07:03.ipv6
URL:http://security.freebsd.org/advisories/FreeBSD-SA-07:03.ipv6.asc

OPENBSD:[3.9] 20070423 012: SECURITY FIX: April 23, 2007
URL:http://openbsd.org/errata39.html#022_route6
OPENBSD:[4.0] 20070423 012: SECURITY FIX: April 23, 2007
URL:http://openbsd.org/errata40.html#012_route6
REDHAT:RHSA-2007:0347
URL:http://www.redhat.com/support/errata/RHSA-2007-0347.html
CERT-VN:VU#267289
URL:http://www.kb.cert.org/vuls/id/267289
BID:23615
URL:http://www.securityfocus.com/bid/23615
FRSIRT:ADV-2007-1563
URL:http://www.frsirt.com/english/advisories/2007/1563
SECTRACK:1017949
URL:http://www.securitytracker.com/id?1017949
SECUNIA:24978
URL:http://secunia.com/advisories/24978
SECUNIA:25033
URL:http://secunia.com/advisories/25033
SECUNIA:25068
URL:http://secunia.com/advisories/25068
SECUNIA:25083
URL:http://secunia.com/advisories/25083
SECUNIA:25288
URL:http://secunia.com/advisories/25288
SECUNIA:25691
URL:http://secunia.com/advisories/25691
SECUNIA:25770
URL:http://secunia.com/advisories/25770
XF:openbsd-ipv6-type0-dos(33851)
URL:http://xforce.iss.net/xforce/xfdb/33851

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2007-2242

- **16543 Linux Kernel error within the "_udp_lib_get_port()" function leading to traffic interception**

A vulnerability has been reported in the Linux Kernel, which potentially can be exploited by malicious, local users to disclose potentially sensitive information.

An error within the "_udp_lib_get_port()" function in net/ipv4/udp.c can be exploited to intercept traffic by binding to a port using a local address if a wildcard bind exists with a local address to that port.

The vulnerability is reported in versions prior to 2.6.21-git8.

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

References:

Original advisory:
http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=de34ed91c4ffa4727964a832c46e624dd1495cf5

Other references:
N.A.

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2007-2480

❖ 16542 Linux Kernel memory leak when releasing PPPoE sockets, Denial of Service Vulnerability

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).

A memory leak exists when releasing PPPoE sockets after they are connected, but before the "PPPIOCGCHAN" ioctl is called. This can be exploited to cause a DoS due to memory exhaustion.

The vulnerability is reported in versions prior to 2.6.21-git8.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/snapshots/patch-2.6.21-git8.log

Other references:
REDHAT:RHSA-2007:0376
URL:https://rhn.redhat.com/errata/RHSA-2007-0376.html
REDHAT:RHSA-2007:0488
URL:http://rhn.redhat.com/errata/RHSA-2007-0488.html
BID:23870
URL:http://www.securityfocus.com/bid/23870
FRSIRT:ADV-2007-1703
URL:http://www.frsirt.com/english/advisories/2007/1703
SECUNIA:25163
URL:http://secunia.com/advisories/25163
SECUNIA:25700
URL:http://secunia.com/advisories/25700
XF:kernel-pppoe-dos(34150)
URL:http://xforce.iss.net/xforce/xfdb/34150

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2007-2525

❖ 16541 Linux Kernel GEODE-AES Encryption Security Issue

A security issue has been reported in the Linux Kernel, which can be exploited by malicious people to disclose potentially sensitive information.

The security issue is caused due to the AMD GEODE-AES driver not correctly setting the encryption key. This results in a weak encryption, which can be exploited to disclose potentially sensitive information.

The vulnerability is reported in versions prior to 2.6.21.3.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.21.3
http://lwn.net/Articles/235711/

Other references:
UBUNTU:USN-470-1
URL:http://www.ubuntu.com/usn/usn-470-1
BID:24150
URL:http://www.securityfocus.com/bid/24150
FRSIRT:ADV-2007-1987
URL:http://www.frsirt.com/english/advisories/2007/1987
SECUNIA:25398
URL:http://secunia.com/advisories/25398
SECUNIA:25596
URL:http://secunia.com/advisories/25596

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2007-2451

❖ 16540 Linux Kernel random number generator to weak the security of applications

A vulnerability has been reported in the Linux Kernel, which can be exploited by malicious, local users to disclose sensitive information.

The kernel does not handle seeds for the random number generator correctly. This may weaken the security of applications relying on the randomness of the kernel random number generator.

The vulnerability is reported in versions prior to 2.6.20.13 or 2.6.21.4.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.21.4

Other references:
MLIST:[linux-kernel] 20070608 Linux 2.6.20.13
URL:http://marc.info/?l=linux-kernel&m=118128610219959&w=2
MLIST:[linux-kernel] 20070608 Linux 2.6.21.4
URL:http://marc.info/?l=linux-kernel&m=118128622431272&w=2
REDHAT:RHSA-2007:0376
URL:https://rhn.redhat.com/errata/RHSA-2007-0376.html
UBUNTU:USN-470-1
URL:http://www.ubuntu.com/usn/usn-470-1
BID:24390
URL:http://www.securityfocus.com/bid/24390
FRSIRT:ADV-2007-2105
URL:http://www.frsirt.com/english/advisories/2007/2105
SECTRACK:1018248
URL:http://www.securitytracker.com/id?1018248
SECUNIA:25596
URL:http://secunia.com/advisories/25596
SECUNIA:25700
URL:http://secunia.com/advisories/25700
XF:kernel-randomnumber-weak-security(34781)
URL:http://xforce.iss.net/xforce/xfdb/34781

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2007-2453

❖ 16539 Linux Kernel underflow error within the "cpuset_task_read()", Information Disclosure Vulnerability

A vulnerability has been reported in the Linux Kernel, which can be exploited by malicious, local users to disclose sensitive information.

An underflow error within the "cpuset_task_read()" function in /kernel/cpuset.c can be exploited to read kernel memory, which may contain potentially sensitive information.

Successful exploitation requires that the attacker has access to open the /dev/cpuset/tasks file (the cpuset file system needs to be mounted).

The vulnerability is reported in versions prior to 2.6.20.13 or 2.6.21.4.

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

References:

Original advisory:
IDEFENSE:20070607 Linux Kernel cpuset tasks Information Disclosure Vulnerability
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=541

Other references:
CONFIRM: http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.20.13
CONFIRM: http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.21.4
BID:24389
URL:http://www.securityfocus.com/bid/24389
FRSIRT:ADV-2007-2105
URL:http://www.frsirt.com/english/advisories/2007/2105
SECTRACK:1018211
URL:http://www.securitytracker.com/id?1018211
XF:kernel-cpusettasksread-info-disclosure(34779)
URL:http://xforce.iss.net/xforce/xfdb/34779

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2007-2875

❖ 16538 Linux Kernel NULL-pointer dereference within netfilter Vulnerability

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

A NULL-pointer dereference exists within netfilter when handling new SCTP connections with unknown chunk types. This can be exploited to crash the kernel by sending malicious packets.

The vulnerability is reported in versions prior to 2.6.20.13 or 2.6.21.4.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.21.4

Other references:
MLIST:[linux-kernel] 20070608 Linux 2.6.20.13
URL:http://marc.info/?l=linux-kernel&m=118128610219959&w=2
MLIST:[linux-kernel] 20070608 Linux 2.6.21.4

URL:http://marc.info/?l=linux-kernel&m=118128622431272&w=2
REDHAT:RHSA-2007:0488
URL:http://rhn.redhat.com/errata/RHSA-2007-0488.html
BID:24376
URL:http://www.securityfocus.com/bid/24376
FRSIRT:ADV-2007-2105
URL:http://www.frsirt.com/english/advisories/2007/2105
XF:kernel-sctpnew-dos(34777)
URL:http://xforce.iss.net/xforce/xfdb/34777

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2007-2876

- **16537 Linux Kernel USBLCD Driver Out of Memory Denial of Service Vulnerability**

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

The USBLCD driver does not limit the memory consumption during writes to the device. This can be exploited to cause an out-of-memory condition by writing a large amount of data to an affected device.

Successful exploitation requires write access to a device using the driver.

The vulnerability is reported in versions prior to 2.6.22-rc7.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.22-rc7

Other references:
* FRSIRT:ADV-2007-2403
* URL:http://www.frsirt.com/english/advisories/2007/2403

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2007-3513

New Vulnerabilities found this Week

HP Instant Support Driver Check sdd.dll Buffer Overflow
"Execution of arbitrary code"

A vulnerability has been reported in HP Instant Support Driver Check, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error when processing the "queryHub()" function in sdd.dll. This can be exploited to cause a buffer overflow via an overly long string passed to the affected function when a user visits a malicious web page.

Successful exploitation allows execution of arbitrary code.

The vulnerability is reported in versions prior to 1.5.0.3.

References:
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01077597
http://www.shinnai.altervista.org/index.php?mod=02_Forum&group=Exploits&argument=Remote&topic=1183360239.ff.php&page=last

Gimp PSD Plugin Integer Overflow Vulnerability
"Execution of arbitrary cod"

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

The vulnerability is caused due to an integer overflow within the function "seek_to_and_unpack_pixeldata()" in plug-ins/common/psd.c. This can be exploited to cause a heap-based buffer overflow by tricking a user into opening a specially crafted PSD file with large width or height values.

Successful exploitation allows execution of arbitrary code.

The vulnerability is confirmed in version 2.2.15. Other versions may also be affected.

References:
http://secunia.com/secunia_research/2007-63/

Firefox "OnKeyDown" Event Focus Weakness
"Disclose sensitive information"

Carl Hardwick has discovered a weakness in Firefox, which potentially can be exploited by malicious people to disclose sensitive information.

The weakness is caused due to a design error within the focus handling of form fields and can potentially be exploited by changing the focus from a "textarea" field to a "file upload" form field via the "OnKeyDown" event.

Successful exploitation allows an arbitrary file on the user's system to be uploaded to a malicious web site, but requires that the user is tricked into typing the file name into a

"textarea" input form.

The weakness is confirmed in version 2.0.0.4. Other versions may also be affected.

References:
http://archives.neohapsis.com/archives/fulldisclosure/2007-06/0646.html

Linux Kernel USBLCD Driver Out of Memory Denial of Service
"Denial of Service"

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

The USBLCD driver does not limit the memory consumption during writes to the device. This can be exploited to cause an out-of-memory condition by writing a large amount of data to an affected device.

Successful exploitation requires write access to a device using the driver.

References:
http://kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.22-rc7

Sun Java Web Start Untrusted Application Arbitrary File Overwrite
"Bypass certain security restrictions"

A vulnerability has been reported in Sun Java Web Start, which can be exploited by malicious people to bypass certain security restrictions.

The vulnerability is caused due to an unspecified error in Java Web Start and can be exploited by an untrusted application to grant itself permissions to overwrite any file that is writable by the user running the application. This can further be exploited to overwrite the user's ".java.policy" file allowing the application to invoke applets or Java Web Start applications.

The vulnerability affects Java Web Start in JDK and JRE 5.0 Update 11 and earlier and Java Web Start in SDK and JRE 1.4.2_13 and earlier for the Windows platform.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102957-1

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