netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 52

December 29, 2006

Table of Contents

Product Focus

Nimda Worm Scanner – The Nimda Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the MS IE Mime Header Flaw (MS01-020) or have been infected by the Nimda Worm.

This Week in Review

Techniques for security testing process. A look inside Vista. Just a little Christmas peace. Let's look at tech trends for 2007.

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

- **Finding software security flaws**

Identify security vulnerabilities in your lab not your customer's production environment
This chapter describes the different analysis techniques you can use during the security testing process. Different situations require different methods of analysis. We also describe the different lab environments that can be set up to perform different types of testing.
White Box Testing
White box testing is common in the quality assurance world. It is sometimes called clear box, open box, or simply informed testing. In white box testing, all information

about the system under test is known to the tester. In the security world, this can also be thought of as an insider attack. The tester has access to the source code and design documentation. This allows the tester to be efficient. He can threat-model the system or do a line-by-line code review, looking for information to guide the selection of test data.

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=development&articleId=9006870&taxonomyId=11&intsrc=kc_feat

❖ Vista's Suicide Bomb: who gets hurt?

Analysis So have fun fighting the battle against CPRM and alike but please do not be surprised when you fail, after all the war has been lost, long live the new world order: proprietary devices, proprietary interfaces, copy protection, limited functionality, and prepare you credit card accounts for all those monthly rental and service charges you will be paying for every "computer controller consumer electronics device" you use.

- Hale Landis, March 2001
If you read just one thing over the holiday break, make sure it's Peter Gutmann's cost analysis of Windows Vista, that we noted here. It's an eye opening 20 minutes.

Gutmann describes in great detail the various measures Microsoft has taken to lock down Windows on behalf of Hollywood. This isn't a comprehensive look at all of Vista's DRM - Gutmann barely touches on Microsoft's new activation framework; this is beyond the scope of his enquiry.)

The Register

Full Story :
http://www.theregister.co.uk/2006/12/28/vista_drm_analysis/

❖ Bot-infected PCs get a refresh

On Christmas day, the number of bots tracked by the Shadowserver group dropped nearly 20 percent.

The dramatic decrease in weekly totals--from more than 500,000 infected systems to less than 400,000 computers--puzzled researchers. The Internet Storm Center, a threat monitoring group managed by the SANS Institute, confirmed a drop of about 10 percent.

One of the Internet Storm Center's network monitoring volunteers posited that the decrease was due to the large number of computers given as gifts this Christmas. The systems running Microsoft Windows XP will be using Service Pack 2, which also means the firewall will be on by default, adding an additional hurdle for bot herder looking to reclaim their drones.

SecurityFocus

Full Story :
http://www.securityfocus.com/brief/395?ref=rss

- **Looking ahead: Tech trends 2007**

On the horizon already: Web 3.0?
As we gaze toward the vista of 2007, we find our e-mail inundated with IT predictions for the new year from analysts, vendors and consultants. From those predictions and our own prognostications we present our forecast for the top IT stories in the year ahead:

Pun aside, Vista

With fanfare, Microsoft Corp. will garner headlines early in the year as it releases its Vista operating system to home users, possibly even at the end of January as currently scheduled, avoiding another delay or three. The release splash will give way to headlines that enterprises are following through on comments from wary IT administrators and are waiting to upgrade. Then will come the security-risk headlines, followed no doubt by the patch headlines.

ComputerWorld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9006579&taxonomyId=17&intsrc=kc_feat

New Vulnerabilities Tested in SecureScout

- **16374 Oracle Linux Kernel "sys_perfmon()" function Denial of Service 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).

The "sys_perfmon()" function on Itanium (IA64) systems does not correctly handle file descriptor reference counts, which can be exploited to cause a DoS by consuming all available file descriptors.

The vulnerability has been reported in versions prior to 2.6.18.

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

References:

Original advisory:
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=b8444d00762703e1b6146fce12ce2684885f8bf6

Other references:
CONFIRM: http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=204360
CONFIRM: http://support.avaya.com/elmodocs2/security/ASA-2006-249.htm
DEBIAN:DSA-1233
URL:http://www.us.debian.org/security/2006/dsa-1233

MANDRIVA:MDKSA-2006:182
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:182
REDHAT:RHSA-2006:0689
URL:http://www.redhat.com/support/errata/RHSA-2006-0689.html
SUSE:SUSE-SA:2006:079
URL:http://www.novell.com/linux/security/advisories/2006_79_kernel.html
BID:20361
URL:http://www.securityfocus.com/bid/20361
FRSIRT:ADV-2006-3937
URL:http://www.frsirt.com/english/advisories/2006/3937
SECUNIA:22279
URL:http://secunia.com/advisories/22279
SECUNIA:22292
URL:http://secunia.com/advisories/22292
SECUNIA:22382
URL:http://secunia.com/advisories/22382
SECUNIA:22945
URL:http://secunia.com/advisories/22945
SECUNIA:23370
URL:http://secunia.com/advisories/23370
XF:kernel-sysperfmon-dos(29384)
URL:http://xforce.iss.net/xforce/xfdb/29384

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-3741

❖ 16375 Linux Kernel "clip_mkip()" function Denial of Service 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).

The "clip_mkip()" function in net/atm/clip.c may dereference a previously freed pointer when processing received data, which can be exploited to cause a kernel panic.

The vulnerability has been reported in versions prior to 2.6.18.

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

References:

Original advisory:
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=fe26109a9dfd9327fdbe630fc819e1b7450986b2

Other references:
CONFIRM: http://support.avaya.com/elmodocs2/security/ASA-2006-249.htm
CONFIRM: http://support.avaya.com/elmodocs2/security/ASA-2006-254.htm
DEBIAN:DSA-1233
URL:http://www.us.debian.org/security/2006/dsa-1233
DEBIAN:DSA-1237

URL:http://www.us.debian.org/security/2006/dsa-1237
MANDRIVA:MDKSA-2006:197
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:197
REDHAT:RHSA-2006:0689
URL:http://www.redhat.com/support/errata/RHSA-2006-0689.html
CONFIRM: http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=206265
REDHAT:RHSA-2006:0710
URL:http://www.redhat.com/support/errata/RHSA-2006-0710.html
SUSE:SUSE-SA:2006:079
URL:http://www.novell.com/linux/security/advisories/2006_79_kernel.html
UBUNTU:USN-395-1
URL:http://www.ubuntu.com/usn/usn-395-1
BID:20363
URL:http://www.securityfocus.com/bid/20363
FRSIRT:ADV-2006-3937
URL:http://www.frsirt.com/english/advisories/2006/3937
FRSIRT:ADV-2006-3999
URL:http://www.frsirt.com/english/advisories/2006/3999
SECUNIA:22253
URL:http://secunia.com/advisories/22253
SECUNIA:22279
URL:http://secunia.com/advisories/22279
SECUNIA:22292
URL:http://secunia.com/advisories/22292
SECUNIA:22497
URL:http://secunia.com/advisories/22497
SECUNIA:22762
URL:http://secunia.com/advisories/22762
SECUNIA:22945
URL:http://secunia.com/advisories/22945
SECUNIA:23064
URL:http://secunia.com/advisories/23064
SECUNIA:23370
URL:http://secunia.com/advisories/23370
SECUNIA:23384
URL:http://secunia.com/advisories/23384
SECUNIA:23395
URL:http://secunia.com/advisories/23395
XF:kernel-clipmkip-dos(29387)
URL:http://xforce.iss.net/xforce/xfdb/29387

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-4997

❖ 16376 Linux Kernel s390 "copy_from_user" Information Disclosure

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

The vulnerability is caused due to the "copy_from_user" function not correctly clearing

kernel buffers after receiving a fault because of invalid user space addresses. This can be exploited to read uninitialized kernel memory by appending to files from invalid addresses.

The vulnerability has been reported in versions prior to 2.6.18.1.

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

References:

Original advisory:
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=52149ba6b0ddf3e9d965257cc0513193650b3ea8
http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.19-rc1

Other references:
MLIST:[linux-kernel] 20061105 Linux 2.6.16.31-rc1
URL:http://lkml.org/lkml/2006/11/5/46
CONFIRM: http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=52149ba6b0ddf3e9d965257cc0513193650b3ea8
CONFIRM: http://support.avaya.com/elmodocs2/security/ASA-2006-254.htm
DEBIAN:DSA-1233
URL:http://www.us.debian.org/security/2006/dsa-1233
DEBIAN:DSA-1237
URL:http://www.us.debian.org/security/2006/dsa-1237
REDHAT:RHSA-2006:0710
URL:http://www.redhat.com/support/errata/RHSA-2006-0710.html
SUSE:SUSE-SA:2006:079
URL:http://www.novell.com/linux/security/advisories/2006_79_kernel.html
BID:20379
URL:http://www.securityfocus.com/bid/20379
FRSIRT:ADV-2006-3938
URL:http://www.frsirt.com/english/advisories/2006/3938
SECTRACK:1017090
URL:http://securitytracker.com/id?1017090
SECUNIA:22289
URL:http://secunia.com/advisories/22289
SECUNIA:22497
URL:http://secunia.com/advisories/22497
SECUNIA:23064
URL:http://secunia.com/advisories/23064
SECUNIA:23370
URL:http://secunia.com/advisories/23370
SECUNIA:23395
URL:http://secunia.com/advisories/23395
XF:kernel-copyfromuser-information-disclosure(29378)
URL:http://xforce.iss.net/xforce/xfdb/29378

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-5174

❖ 16377 Linux Kernel IPv6 Flow Label 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 seqfiles for "/proc/net/ip6_flowlabel", which can be exploited to cause kernel lockups and crashes via specially crafted flow labels.

The vulnerability has been reported in versions prior to 2.6.18.2.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.18.2
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=bcd620757d3a4ae78ef0ca41adb5d9e400ed92b6

Other references:
MLIST:[linux-kernel] 20061105 Linux 2.6.16.31-rc1
URL:http://lkml.org/lkml/2006/11/5/46
CONFIRM: http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=bcd620757d3a4ae78ef0ca41adb5d9e400ed92b6
CONFIRM: https://issues.rpath.com/browse/RPL-760
DEBIAN:DSA-1233
URL:http://www.us.debian.org/security/2006/dsa-1233
SUSE:SUSE-SA:2006:079
URL:http://www.novell.com/linux/security/advisories/2006_79_kernel.html
UBUNTU:USN-395-1
URL:http://www.ubuntu.com/usn/usn-395-1
BID:20847
URL:http://www.securityfocus.com/bid/20847
FRSIRT:ADV-2006-4297
URL:http://www.frsirt.com/english/advisories/2006/4297
SECUNIA:22665
URL:http://secunia.com/advisories/22665
SECUNIA:22754
URL:http://secunia.com/advisories/22754
SECUNIA:23370
URL:http://secunia.com/advisories/23370
SECUNIA:23384
URL:http://secunia.com/advisories/23384
XF:kernel-seqfile-ipv6-dos(29970)
URL:http://xforce.iss.net/xforce/xfdb/29970

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-5619

❖ 16378 Linux Kernel ISO9660 Local Denial of Service

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

The vulnerability is caused due an error within the "grow_buffers()" function when receiving a block number which is outside of the maximum-addressable pagecache range. This can be exploited to cause an infinite loop in the "__getblk_slow()" function by e.g. mounting a specially crafted ISO9660 image and performing a read operation on the mounted file system.

The vulnerability has been reported in versions prior to 2.6.18.2.

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

References:

Original advisory:
http://projects.info-pull.com/mokb/MOKB-05-11-2006.html
http://git.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=e5657933863f43cc6bb76a54d659303dafaa9e58;hp=e0ab2928cc2202f13f0574d4c6f567f166d307eb

Other references:
MISC: http://projects.info-pull.com/mokb/MOKB-05-11-2006.html
SUSE:SUSE-SA:2006:079
URL:http://www.novell.com/linux/security/advisories/2006_79_kernel.html
BID:20920
URL:http://www.securityfocus.com/bid/20920
FRSIRT:ADV-2006-4359
URL:http://www.frsirt.com/english/advisories/2006/4359
SECUNIA:22702
URL:http://secunia.com/advisories/22702
SECUNIA:22746
URL:http://secunia.com/advisories/22746
XF:kernel-iso9660-dos(30029)
URL:http://xforce.iss.net/xforce/xfdb/30029

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-5757

❖ 16379 Linux Kernel Fragmented IPv6 Packet Filtering Bypass

Some vulnerabilities have been reported in the Linux Kernel, which can be exploited by malicious people to bypass certain security restrictions.

The vulnerabilities are caused due to the incorrect processing of certain fragmented IPv6 packets. This can be exploited to bypass filtering rules by sending specially crafted packets.

The vulnerability has been reported in versions prior to 2.6.16.31.

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

References:

Original advisory:
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=51d8b1a65291a6956b79374b6adbbadc2263bcf6
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=6d381634d213580d40d431e7664dfb45f641b884

Other references:
MLIST:[linux-kernel] 20061105 Linux 2.6.16.31-rc1
URL:http://readlist.com/lists/vger.kernel.org/linux-kernel/55/275979.html
CONFIRM: http://www.kernel.org/git/?p=linux%2Fkernel%2Fgit%2Fstable%2Flinux-2.6.16.y.git&a=search&s=CVE-2006-4572
CONFIRM: http://www.kernel.org/git/?p=linux/kernel/git/stable/linux-2.6.16.y.git;a=commit;h=0ddfcc96928145d6a6425fdd26dad6abfe7f891d
CONFIRM: http://www.kernel.org/git/?p=linux/kernel/git/stable/linux-2.6.16.y.git;a=commit;h=6ac62be885810e1f8390f0c3b9d3ee451d3d3f19
CONFIRM: http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.31
MANDRIVA:MDKSA-2006:197
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:197
SUSE:SUSE-SA:2006:079
URL:http://www.novell.com/linux/security/advisories/2006_79_kernel.html
UBUNTU:USN-395-1
URL:http://www.ubuntu.com/usn/usn-395-1
BID:20955
URL:http://www.securityfocus.com/bid/20955
FRSIRT:ADV-2006-4386
URL:http://www.frsirt.com/english/advisories/2006/4386
SECUNIA:22731
URL:http://secunia.com/advisories/22731
SECUNIA:22762
URL:http://secunia.com/advisories/22762
SECUNIA:23384
URL:http://secunia.com/advisories/23384

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-4572

❖ 16380 Linux Kernel "get_fdb_entries()" Integer Overflow Vulnerability

Eugene Teo has reported a vulnerability in the Linux Kernel, which potentially can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to an integer overflow within the "get_fdb_entries()" function in net/bridge/br_ioctl.c. This can be exploited to cause a buffer overflow via specially crafted ioctl() requests.

Successful exploitation may allow the execution of arbitrary code with escalated privileges.

The vulnerability has been reported in versions prior to 2.6.18.4.

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

References:

Original advisory:
http://projects.info-pull.com/mokb/MOKB-29-11-2006.html
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.18.4

Other references:
BUGTRAQ:20061206 rPSA-2006-0226-1 kernel
URL:http://www.securityfocus.com/archive/1/archive/1/453681/100/0/threaded
MISC: http://projects.info-pull.com/mokb/MOKB-29-11-2006.html
MISC: http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=blobdiff;h=4c61a7e0a86e1ae9e16867f9f8e4b0412b8edbaf;hp=4e4119a1213925568b8a1acdef9bf52b98b19da3;hb=ba8379b220509e9448c00a77cf6c15ac2a559cc7;f=net/bridge/br_ioctl.c
CONFIRM: http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=ba8379b220509e9448c00a77cf6c15ac2a559cc7
CONFIRM: http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.18.4
CONFIRM: https://issues.rpath.com/browse/RPL-803
CONFIRM: https://issues.rpath.com/browse/RPL-837
DEBIAN:DSA-1233
URL:http://www.us.debian.org/security/2006/dsa-1233
SUSE:SUSE-SA:2006:079
URL:http://www.novell.com/linux/security/advisories/2006_79_kernel.html
UBUNTU:USN-395-1
URL:http://www.ubuntu.com/usn/usn-395-1
BID:21353
URL:http://www.securityfocus.com/bid/21353
FRSIRT:ADV-2006-4781
URL:http://www.frsirt.com/english/advisories/2006/4781
SECUNIA:23073
SECUNIA:23252
URL:http://secunia.com/advisories/23252
SECUNIA:23370
URL:http://secunia.com/advisories/23370
SECUNIA:23384
URL:http://secunia.com/advisories/23384
XF:linux-getfdbentries-integer-overflow(30588)
URL:http://xforce.iss.net/xforce/xfdb/30588

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-5751

❖ 16381 Linux Kernel "ip_summed" Memory Corruption Vulnerability

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

The vulnerability is caused due to a memory corruption in

drivers/net/tokenring/ibmtr.c, which can be exploited to cause a DoS by sending specially crafted packet to a vulnerable system.

The vulnerability is reported in Linux Kernel 2.6.19.

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

References:

Original advisory:
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=ee28b0da1069ced1688aa9d0b7b378353b988321

Other references:
CONFIRM: http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=ee28b0da1069ced1688aa9d0b7b378353b988321
CONFIRM: http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=blobdiff;h=0d97e10ccac580e16d3dffbe4a9a88144360e64a;hp=bfe59865b1dd50e5c4dbd4cefe506a31e1495a1a;hb=ee28b0da1069ced1688aa9d0b7b378353b988321;f=drivers/net/tokenring/ibmtr.c
BID:21490
URL:http://www.securityfocus.com/bid/21490
FRSIRT:ADV-2006-4907
URL:http://www.frsirt.com/english/advisories/2006/4907
SECUNIA:23254
URL:http://secunia.com/advisories/23254

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-6333

❖ 16382 Linux Kernel "nlmclnt_mark_reclaim()" function 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 within the "nlmclnt_mark_reclaim()" function in clntlock.c of the NFS lockd can be exploited by malicious people to cause a DoS by crashing the service.

The vulnerability is reported in Linux Kernel 2.6.16.

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

References:

Original advisory:
http://www.ubuntu.com/usn/usn-395-1
http://www.us.debian.org/security/2006/dsa-1233

Other references:

MLIST:[linux-kernel] 20051216 lockd: couldn't create RPC handle for (host)
URL:http://marc.theaimsgroup.com/?l=linux-kernel&m=113476665626446&w=2
MLIST:[linux-kernel] 20051218 Re: lockd: couldn't create RPC handle for (host)
URL:http://marc.theaimsgroup.com/?l=linux-kernel&m=113494474208973&w=2
CONFIRM: http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=9b5b1f5bf9dcdb6f23abf65977a675eb4deba3c0
SUSE:SUSE-SA:2006:057
URL:http://www.novell.com/linux/security/advisories/2006_57_kernel.html
UBUNTU:USN-395-1
URL:http://www.ubuntu.com/usn/usn-395-1
SECUNIA:23361
URL:http://secunia.com/advisories/23361
SECUNIA:23384
URL:http://secunia.com/advisories/23384

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-5158

❖ 16383 Linux Kernel task switching implementation failure to save and restore EFLAGS of process, Application Crash

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

The task switching implementation fails to save and restore EFLAGS of process correctly. This can be exploited by malicious, local users to crash applications and services by invoking a specially crafted executable.

The vulnerability is reported in Linux Kernel 2.6.16.

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

References:

Original advisory:
http://www.ubuntu.com/usn/usn-395-1
http://www.us.debian.org/security/2006/dsa-1233

Other references:
CONFIRM: http://kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=47a5c6fa0e204a2b63309c648bb2fde36836c826
SUSE:SUSE-SA:2006:079
URL:http://www.novell.com/linux/security/advisories/2006_79_kernel.html
UBUNTU:USN-395-1
URL:http://www.ubuntu.com/usn/usn-395-1
SECUNIA:23361
URL:http://secunia.com/advisories/23361
SECUNIA:23384
URL:http://secunia.com/advisories/23384

Product Homepage:

http://kernel.org/

CVE Reference: CVE-2006-5173

New Vulnerabilities found this Week

Novell NetMail NMAP/IMAP Multiple Vulnerabilities

"Denial of Service"

Some vulnerabilities have been reported in Novell NetMail, which can be exploited by malicious users to cause a DoS (Denial of Service) or compromise a vulnerable system and by malicious people to compromise a vulnerable system.

1) A boundary error within the NMAP (Network Messaging Application Protocol) service when handling STOR commands can be exploited to cause a buffer overflow by passing an overly long argument to the command.

Successful exploitation requires a valid user account.

2) A boundary error in the IMAP service when handling the SUBSCRIBE command can be exploited to cause a stack-based buffer overflow by passing an overly long string as argument.

Successful exploitation requires a valid user account.

3) An unspecified error in the IMAP service when handling the APPEND command can be exploited to cause a DoS.

Successful exploitation requires a valid user account.

4) An input validation error in the IMAP service when processing command continuation requests can be exploited to cause a heap-based buffer overflow.

5) A boundary error in the IMAP service when handling the APPEND command can be exploited to cause a stack-based buffer overflow by passing a specially crafted, overly long argument to the command.

Successful exploitation requires a valid user account.

The vulnerabilities are reported in version 3.5.2. Other versions may also be affected.

References:
https://secure-support.novell.com/KanisaPlatform/Publishing/134/3096026_f.SAL_Public.html
https://secure-support.novell.com/KanisaPlatform/Publishing/328/3717068_f.SAL_Public.html
http://www.zerodayinitiative.com/advisories/ZDI-06-052.html
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=454
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=455

Oracle Portal Multiple Vulnerabilities

"HTTP response splitting and cross-site scripting attacks"

putosoft softputo has reported some vulnerabilities in Oracle Portal, which can be exploited by malicious people to conduct HTTP response splitting and cross-site scripting attacks.

1) Input passed to the "enc" parameter in webapp/jsp/calendar.jsp, webapp/jsp/calendarDialog.jsp, and webapp/jsp/fred.jsp is not properly sanitized before being returned to the user. This can be exploited to insert arbitrary HTTP headers, which are included in the response to the sender.

2) Various input (e.g. the "tc" parameter in webapp/jsp/container_tabs.jsp) is not properly sanitized before being returned to users. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site.

References:
http://lists.grok.org.uk/pipermail/full-disclosure/2006-December/051380.html

Sun Solaris WAN Boot RSA Signature Forgery Vulnerability
"Bypass security restrictions"

Sun has acknowledged a vulnerability in Solaris, which can be exploited by malicious people to bypass certain security restrictions.

The vulnerability is caused due to the WAN Boot software using a static version of a vulnerable OpenSSL library.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102759-1

SGI Advanced Linux Environment Multiple Updates
"Bypass security restrictions"

SGI has issued a patch for SGI Advanced Linux Environment. This fixes some vulnerabilities, which can be exploited by malicious people to bypass certain security restrictions and compromise a vulnerable system.

References:
ftp://patches.sgi.com/support/free/security/advisories/20061201-01-P.asc

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