ScoutNews Team **March 10, 2006**
2006 Issue # 10

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review
Top Security News Stories this Week
New Test Cases Tested in SecureScout
New Vulnerabilities this Week

New in SecureScout

A new Sarbanes-Oxley SafeScan policy for SecureScout was released, adding to the existing SafeScan policies for HIPAA and GLBA. (read press release)

Product Spotlight: Apache Chunked Vulnerability Scanner - Free SecureScout single scanner. Quickly experience the power of SecureScout in testing for Chunked Encoding buffer overflow in Apache web servers.

This Week in Review

Worms in the apples, Hack for hire sites shut down, Symantec quietly exits the password cracker business and security advice from the Yankee Group.

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

- **Apple releases bushel of bug fixes**

The last 2 weeks have been tough on those Apple fans that have proclaimed that the Mac is invulnerable to hacker virus' and worms. These past 14 days have seen the emergence of roughly 20 vulnerabilities identified in the 'invulnerable' Mac OS X.

Apple may have to increase the frequency of patch releases from every 2 months; especially since the introduction of Intel-based systems that will be victim to more 'portable' exploits.

Full Story :
http://www.redherring.com/Article.aspx?a=15933&hed=Apple+Patches+Security+Flaws&sector=Industries&subsector=SecurityAndDefense

❖ Hack-for-sale website shut down

As reported in ScoutNews last week(issue 2006 #9), a company calling itself PandaLabs was purveying Trojan generation software Briz.a.

Five websites were shuttered in a cooperative effort between Panda Software (a very reputable Spanish company) and RSA Security.
TechWeb News

Full Story :
http://www.smallbizpipeline.com/181502002?cid=rssfeed_pl_sbp

❖ Symantec halts sales of L0phtCrack

Symantec quietly discontinued sales of the "password auditing and recovery application" this week. Symantec gained LOphtCrack through the acquisition of @Stake in 2004. @Stake sold the password cracker under the moniker LC4

It was not made immediately clear why Symantec has chosen to no longer support LOphtCrack.

Related Links :
http://www.aviransplace.com/index.php/archives/2006/03/09/symantec-pulls-plug-on-l0phtcrack/

❖ Yankee analyst speaks on information security

Andrew Jaquith with the Yankee Group dispenses some advice on protecting vital corporate information. Make security data centric; that is set the policies based on the type of information to be protected versus a blanket approach for all data.

Mr. Jaquith also touches on the risks posed by outsourcing both IT service and personnel.

ContactCenterToday

Related Links :
http://www.contact-center-today.com/story.xhtml?story_id=41887

New Vulnerabilities Tested in SecureScout

- **16149 Linux Kernel "die_if_kernel()" Potential 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).

The vulnerability is caused due to the "die_if_kernel()" function in "arch/ia64/kernel/unaligned.c" being erroneously marked with a "noreturn" attribute. This can potentially be exploited to cause a DoS on Itanium systems, when the kernel is compiled with certain version of the gcc compiler.

The vulnerability affects versions 2.6 through 2.6.15.6 not included.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.15.6

Other references:
http://secunia.com/advisories/19078/

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2006-0742

- **16150 Linux Kernel validation error in "/fs/nfsd/nfs2acl.c" to set ACLs on NFS filesystems Vulnerability**

A vulnerability has been reported in the Linux Kernel, which potentially can be exploited by malicious, local users to bypass certain security restrictions.

A validation error in "/fs/nfsd/nfs2acl.c" may be exploited by malicious users to set ACLs on NFS filesystems even when the filesystems are exported read-only.

The vulnerability affects versions 2.6 through 2.6.15 not included.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.14.5

Other references:
http://secunia.com/advisories/18216/
* MISC:http://lkml.org/lkml/2005/12/23/171
* SUSE:SuSE-SA:2006:006
* URL:http://www.novell.com/linux/security/advisories/2006_06_kernel.html
* SECUNIA:18788
* URL:http://secunia.com/advisories/18788

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-3623

❖ 16151 Linux Kernel "/sys/module/drm/parameters/debug" file created with world-writable permission in sysfs Vulnerability

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

The "/sys/module/drm/parameters/debug" file is created with world-writable permission in sysfs. This may be exploited by non-privileged users to turn on drm debugging.

The vulnerability affects versions 2.6 through 2.6.13.4 not included.

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

References:

Original advisory:
http://www.kernel.org/hg/linux-2.6/?cmd=changeset;node=d7067d7d1f92cba14963a430cfbd53098cbbc8fd

Other references:
* CONFIRM:http://bugs.gentoo.org/show_bug.cgi?id=107893
* FEDORA:FEDORA-2005-1007
* URL:http://www.securityfocus.com/advisories/9549
* MANDRAKE:MDKSA-2005:220
* URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:220
* MANDRIVA:MDKSA-2005:220
* URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:220
* MANDRIVA:MDKSA-2005:235
* URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:235
* BID:15154
* URL:http://www.securityfocus.com/bid/15154

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-3179

❖ 16152 Linux Kernel Session Keyring Allocation Local Denial of Service Vulnerability

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

An error within the error handling path for the "KEYCTL_JOIN_SESSION_KEYRING" operation when attempting to join a key management session may cause the session management semaphore to not be released. This can be exploited by attempting to add a new session keyring.

The vulnerability affects versions 2.6 through 2.6.13.4 not included.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12.5

Other references:
* CONFIRM:http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12.5
* MANDRAKE:MDKSA-2005:220
* URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:220
* MANDRIVA:MDKSA-2005:220
* URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:220
* UBUNTU:USN-169-1
* URL:http://www.ubuntulinux.org/support/documentation/usn/usn-169-1
* BID:14521
* URL:http://www.securityfocus.com/bid/14521
* SECUNIA:16355
* URL:http://secunia.com/advisories/16355/

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-2098

❖ 16153 Linux Kernel "sys_mbind()" function to cause a local DoS Vulnerability

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

The "sys_mbind()" function does not sanity check its arguments, which potentially can be exploited to cause a local DoS.

The vulnerability affects versions 2.6 through 2.6.15.5 not included.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.15.5

Other references:
http://secunia.com/advisories/19083/

Product HomePage:
http://kernel.org/

CVE Reference: None

❖ 16154 Linux Kernel ELF Core Dump Privilege Escalation Vulnerability

Paul Starzetz has reported a vulnerability in the Linux kernel, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to a signedness error in the Linux ELF binary format loader's core dump function (elf_core_dump()) and can be exploited to cause a buffer overflow via a specially crafted ELF binary.

Successful exploitation makes it possible to gain root privileges and execute arbitrary code with kernel privileges.

The vulnerability has been reported in versions 2.2 through 2.2.27-rc2, versions 2.4 through 2.4.31-pre1, and versions 2.6 through 2.6.12-rc4.

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

References:

Original advisory:

http://www.isec.pl/vulnerabilities/isec-0023-coredump.txt

http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11.9

Other references:

* BUGTRAQ:20050511 Linux kernel ELF core dump privilege elevation

* URL:http://www.securityfocus.com/archive/1/397966

* MISC:http://www.isec.pl/vulnerabilities/isec-0023-coredump.txt

* FRSIRT:ADV-2005-0524

* URL:http://www.frsirt.com/english/advisories/2005/0524

* OVAL:OVAL1122

* URL:http://oval.mitre.org/oval/definitions/data/oval1122.html

Product HomePage:

http://kernel.org/

CVE Reference: CVE-2005-1263

❖ 16155 Linux Kernel sysfs file "alarms" with insecure permissions to cause 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 it87 and via686a hardware monitoring drivers create the sysfs file "alarms" with insecure permissions granting write access to the file. This can be exploited to exhaust all available CPU resources by writing to the file.

The vulnerability has been reported in versions 2.6 through 2.6.11.8.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Medium** Risk: **DoS, 100% CPU**

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11.8

Other references:
* CONFIRM:http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11.8
* CONFIRM:http://lkml.org/lkml/2005/4/20/159

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-1369

❖ 16156 Linux Kernel "key_user_lookup()" to crash the kernel Vulnerability

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

An error in the "key_user_lookup()" function in "security/keys/key.c" can be exploited to crash the kernel.

The vulnerability has been reported in versions 2.6 through 2.6.11.8

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11.8

Other references:
* CONFIRM:http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11.8
* CONFIRM:http://linux.bkbits.net:8080/linux-2.6/cset%40423078fafVa6mAyny23YZ87hDipmTw

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-1368

❖ 16157 Linux Kernel "is_hugepage_only_range()" Denial of Service Vulnerability

Daniel McNeil 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 to an error in the AIO (Asynchronous I/O) support within the "is_hugepage_only_range()" function. This can be exploited via a specially crafted program calling the "io_queue_init()" function and then exiting without calling the "io_queue_release()" function.

Successful exploitation crashes the system on PPC64 and IA64 architectures, but requires that CONFIG_HUGETLB_PAGE is enabled.

The vulnerability has been reported in versions 2.6.8 and 2.6.11. Other versions may also be affected.

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

References:

Original advisory:
http://linux.bkbits.net:8080/linux-2.6/cset%404248c8c0es30_4YVdwa6vteKi7h_nw

Other references:
* MISC:http://groups-beta.google.com/group/linux.kernel/browse_thread/thread/13b43bd5783842f6/7ce3c5a514a497ab?q=io_queue_init&rnum=3#7ce3c5a514a497ab
* CONFIRM:http://linux.bkbits.net:8080/linux-2.6/cset%404248c8c0es30_4YVdwa6vteKi7h_nw
* SUSE:SUSE-SA:2005:050
* URL:http://www.novell.com/linux/security/advisories/2005_50_kernel.html

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-0916

❖ 16158 Linux Kernel ISO9660 filesystem handler to cause DoS Vulnerability

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

a DoS (Denial of Service) or potentially corrupt memory leading to execution of arbitrary code.

Some unspecified errors have been reported in the ISO9660 filesystem handler including Rock Ridge and Juliet extensions. These can be exploited via a specially crafted filesystem to cause a DoS or potentially corrupt memory leading to execution of arbitrary code.

The vulnerability has been reported in versions 2.6 through 2.6.11.6.

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

Other references:
* BUGTRAQ:20050317 Linux ISO9660 handling flaws
* URL:http://www.securityfocus.com/archive/1/393590
* CONFIRM:http://kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.12-rc1
* 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
* BID:12837
* URL:http://www.securityfocus.com/bid/12837
* SECUNIA:18684
* URL:http://secunia.com/advisories/18684
* XF:kernel-iso9660-filesystem(19741)
* URL:http://xforce.iss.net/xforce/xfdb/19741

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-0815

New Vulnerabilities found this Week

SGI Advanced Linux Environment Multiple Updates
"Denial of Service"

SGI has issued a patch for SGI Advanced Linux Environment. This fixes some vulnerabilities, which can be exploited by malicious people to cause a DoS (Denial of Service), cause files to be extracted to arbitrary locations on a user's system, and potentially compromise a user's system.

References:
ftp://patches.sgi.com/support/free/security/advisories/20060301-01.U.asc

Gallery "stepOrder[]" Local File Inclusion Vulnerability
"Disclose sensitive information"

rgod has discovered a vulnerability in Gallery, which can be exploited by malicious people to disclose sensitive information and compromise a vulnerable system.

Input passed to the "stepOrder[]" parameter in "upgrade/index.php" and "install/index.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from local resources.

Successful exploitation requires that "magic_quotes_gpc" is disabled and that "register_globals" is enabled.

This can further be exploited to include arbitrary PHP code injected into "g2data/plugins_data/modules/watermark".

The vulnerability has been confirmed in version 2.0.3 and has also been reported in prior versions. Other versions may also be affected.

References:
http://milw0rm.com/exploits/1566

Symantec Ghost Multiple Vulnerabilities
"Gain knowledge of potentially sensitive information; Modify data; Gain escalated privileges"

Three vulnerabilities have been reported in Symantec Ghost, which can be exploited by malicious, local users to gain knowledge of potentially sensitive information, modify certain data, and potentially gain escalated privileges.

1) Default administrator login id and password left behind during installation can be used by local users to modify or delete stored administrative tasks. This can be exploited to modify tasks to run arbitrary code on the local system.

2) Insecure permissions in the shared memory sections within the Sybase SQLAnywhere database used by Symantec Ghost can potentially be exploited to gain access to, and to modify information stored in the database.

3) A boundary error in the login dialog box of dbisqlc.exe which is installed as a part of the SQLAnywhere package, can cause a buffer overflow. This can potentially be exploited to gain access to information stored in the database that is not normally accessible.

The vulnerabilities have been reported in the following versions:
* Symantec Ghost 8.0.
* Symantec Ghost 8.2 (shipped as a part of Symantec Ghost Solutions Suite 1.0).

References:
http://securityresponse.symantec.com/avcenter/security/Content/2006.03.07.html

Linux Kernel "die_if_kernel()" Potential Denial of Service
"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 the "die_if_kernel()" function in "arch/ia64/kernel/unaligned.c" being erroneously marked with a "noreturn" attribute. This can potentially be exploited to cause a DoS on Itanium systems, when the kernel is compiled with certain version of the gcc compiler.

References:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.15.6

Sun Solaris "/proc" Denial of Service Vulnerability
"Denial of Service"

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

The vulnerability is caused due to an unspecified error within the pagedata subsystem of the process file system "/proc". This can be exploited by an unprivileged user to cause the system to become unresponsive, and resulting in a DoS.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102159-1

LISTSERV WA CGI Script Buffer Overflow Vulnerabilities
"Buffer overflows**"**

Peter Winter-Smith of NGSSoftware has reported some vulnerabilities in LISTSERV, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerabilities are caused due to some unspecified boundary errors in the WA CGI script and can be exploited to cause buffer overflows.

Successful exploitation allows execution of arbitrary code.

The vulnerabilities have been reported in versions 14.3 and 14.4. Prior versions may also be affected.
References:
http://www.ngssoftware.com/advisories/listserv_3.txt
http://www.kb.cert.org/vuls/id/841132

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