netVigilance

ScoutNews

April 7, 2006
2006 Issue # 14

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Top Virus list out for March, HP printers pose threat to PCs, Hackers resort to new tactics to stay hidden and Botnet farms attacking Internet hosts.

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

❖ List of top virus' and hoaxes for March '06

Sophos has compiled it's list of the top 10 Virus' and email hoaxes for March. The Virus list is dominated by some old familiar names, with a newcomer making a strong charge to 6th; the Clagger-I Trojan.

The email hoax list is more interesting, while the number of viral email messages has dropped to a mere 0.9%; the real threat from email is now of course phishing. (What, Do you mean that Bill Gates is not giving away his fortune? – *Ed.*)

infoZine

Full Story:
http://www.infozine.com/news/stories/op/storiesView/sid/14081/

❖ HP Printer vulnerability threatens PC hard drives

Certain business class Laserjet printers from HP contain a vulnerability that could allow a hacker to gain access to the PCs connected to the printers. Color LaserJet 2500 and Color LaserJet 4600 printers install an HTTP server on the connected PC used for remotely monitoring and changing printer settings.

The toolbox software included with the printers that contains the flaw, can be patched by visiting this HP support site:

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00634759&printver=true
TechWeb.com

Full Story:
http://www.channelweb.com/sections/allnews/article.jhtml?articleId=184429372

❖ Hackers using security vendors, each other to launch attacks.

Kaspersky Labs recently detected a trend where hackers launch attacks against Honeypots at security firms as well as other hackers in order to create a ‘smoke screen’ to cover up their nefarious activities.

Kaspersky found that more savvy hackers will launch DoS attacks against Honeypots, intentionally avoid IP addresses of security companies and pirate other hackers botnet machines to launch attacks.

All of these tactics are attempts to launch new attacks completely undetected. By tying up or avoiding Honeypot networks, the hackers can operate in the wild a lot longer before the security vendors release detection rules.
CNET

Full Story :
http://news.com.com/2100-7349_3-6057654.html

❖ Sharp rise in DDoS against internet DNS infrastructure

The .com name servers and other pieces of the Internet infrastructure are being bombarded with a new virulent form of DDoS attacks known as DNS amplification.

According to a report of ICANN's Security and Stability Advisory Committee, published late Friday, there was an attack against a “key TLD [top-level domain] name server operator” on February 5. The aggregate bandwidth deployed against the target was 1Gbps.

Datamonitor

Full Story:
http://www.computerwire.com/industries/research/?pid=06EA389F-49D7-48B4-A856-17974DAC28F6

New Vulnerabilities Tested in SecureScout

❖ 16190 Microsoft Internet Explorer Window Loading Race Condition Address Bar Spoofing (Remote File Checking)

Hai Nam Luke has discovered a vulnerability in Internet Explorer, which can be exploited by malicious people to conduct phishing attacks.

The vulnerability is caused due to a race condition in the loading of web content and Macromedia Flash Format files (".swf") in browser windows. This can be exploited to spoof the address bar in a browser window showing web content from a malicious web site.

The vulnerability has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP1/SP2. The vulnerability has also been confirmed in Internet Explorer 7 Beta 2 Preview (March edition). Other versions may also be affected.

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

References:

Original advisory:
BUGTRAQ:20060403 Another Internet Explorer Address Bar Spoofing Vulnerability
URL:http://www.securityfocus.com/archive/1/archive/1/429719/100/0/threaded

Other references:
http://secunia.com/advisories/19521/

CVE Reference: CVE-2006-1626

❖ 16191 Linux Kernel "sys_epoll_wait()" Function Integer Overflow

Georgi Guninski has reported a potential vulnerability in the Linux kernel, which may be exploited by malicious people to gain escalated privileges.

The vulnerability is caused due to an integer overflow in the "sys_epoll_wait()" function and can be exploited to cause a buffer overflow overwriting low kernel memory.

Successful exploitation may potentially allow execution of arbitrary code with escalated privileges. However, few applications reportedly use the affected part of the kernel memory space.

The vulnerability has been reported in versions 2.6 through 2.6.11.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11.2

Other references:
* FULLDISC:20050309 overwriting low kernel memory
* URL:http://lists.grok.org.uk/pipermail/full-disclosure/2005-March/032314.html
* CONFIRM:http://linux.bkbits.net:8080/linux-2.6/cset@422dd06a1p5PsyFhoGAJseinjEq3ew?nav=index.html|ChangeSet@-1d
* REDHAT:RHSA-2005:293
* URL:http://www.redhat.com/support/errata/RHSA-2005-293.html
* REDHAT:RHSA-2005:366
* URL:http://www.redhat.com/support/errata/RHSA-2005-366.html
* SUSE:SUSE-SA:2005:018
* URL:http://www.novell.com/linux/security/advisories/2005_18_kernel.html
* UBUNTU:USN-95-1
* URL:http://www.ubuntulinux.org/support/documentation/usn/usn-95-1
* BID:12763
* URL:http://www.securityfocus.com/bid/12763

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2005-0736

❖ 16192 Linux Kernel "shmctl()" function to disclose sensitive information

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

Insufficient permission checking in the "shmctl()" function allows any process to lock/unlock arbitrary System V shared memory segments that fall within the RLIMIT_MEMLOCK limit.

This can be exploited to unlock locked memory of other processes, which may result in sensitive information being written to swap space.

The vulnerability has been reported in versions 2.6 through 2.6.11.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11

Other references:
* BUGTRAQ:20050215 [USN-82-1] Linux kernel vulnerabilities
* URL:http://marc.theaimsgroup.com/?l=full-disclosure&m=110846102231365&w=2
* CONECTIVA:CLA-2005:930
* URL:http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000930
* REDHAT:RHSA-2005:092
* URL:http://www.redhat.com/support/errata/RHSA-2005-092.html
* REDHAT:RHSA-2005:472
* URL:http://www.redhat.com/support/errata/RHSA-2005-472.html
* OVAL:OVAL1225
* URL:http://oval.mitre.org/oval/definitions/data/oval1225.html

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2005-0176

❖ 16193 Linux Kernel race condition exists in the terminal handling of the "setsid()" function

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

A race condition exists in the terminal handling of the "setsid()" function used for starting new process sessions.

The vulnerability has been reported in versions 2.6 through 2.6.11.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11

Other references:
* CONFIRM:http://linux.bkbits.net:8080/linux-2.6/cset@41ddda70CWJb5nNL71T4MOlG2sMG8A
* CONECTIVA:CLA-2005:930
* URL:http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000930
* REDHAT:RHSA-2005:092
* URL:http://www.redhat.com/support/errata/RHSA-2005-092.html
* BUGTRAQ:20050215 [USN-82-1] Linux kernel vulnerabilities
* URL:http://marc.theaimsgroup.com/?l=full-disclosure&m=110846102231365&w=2

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2005-0178

❖ 16194 Linux Kernel error within the handling of the OUTS instruction to allow local users to write to privileged IO ports

A vulnerability has been reported in the Linux kernel and can be exploited by malicious, local users to bypass security restrictions.

An error within the handling of the OUTS instruction on 64-bit platforms can be exploited by malicious, local users to write to privileged IO ports.

The vulnerability has been reported in versions 2.6 through 2.6.8.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.9

Other references:
* REDHAT:RHSA-2005:092
* URL:http://www.redhat.com/support/errata/RHSA-2005-092.html
* REDHAT:RHSA-2005:293
* URL:http://www.redhat.com/support/errata/RHSA-2005-293.html

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2005-0204

❖ 16195 Linux Kernel Table sizes in "nls_ascii.c" to be exploited to cause buffer overflows and crash the kernel

A vulnerability has been reported in the Linux kernel and can be exploited by malicious, local users to cause buffer overflows and crash the kernel.

Table sizes in "nls_ascii.c" are incorrectly set to 128 instead of 256, which may be exploited to cause buffer overflows and crash the kernel.

The vulnerability has been reported in versions 2.6 through 2.6.11.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11

Other references:
* CONFIRM:http://linux.bkbits.net:8080/linux-2.6/cset@41e2bfbeOiXFga62XrBhzm7Kv9QDmQ
* CONECTIVA:CLA-2005:930
* URL:http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000930
* REDHAT:RHSA-2005:092
* URL:http://www.redhat.com/support/errata/RHSA-2005-092.html
* BUGTRAQ:20050215 [USN-82-1] Linux kernel vulnerabilities
* URL:http://marc.theaimsgroup.com/?l=full-disclosure&m=110846102231365&w=2

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2005-0177

❖ 16196 Linux Kernel design error in the netfilter/iptables module to be exploited to crash the kernel or bypass firewall rules

A vulnerability has been reported in the Linux kernel and can be exploited by malicious users to crash the kernel or bypass firewall rules via specially crafted packets.

A design error in the netfilter/iptables module can be exploited to crash the kernel or bypass firewall rules via specially crafted packets.

The vulnerability has been reported in versions 2.6 through 2.6.11.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11

Other references:
* MLIST:[netdev] 20050124 Re: skb_checksum_help
* URL:http://oss.sgi.com/archives/netdev/2005-01/msg01036.html
* CONECTIVA:CLA-2005:945
* URL:http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000945
* DEBIAN:DSA-1017
* URL:http://www.debian.org/security/2006/dsa-1017
* DEBIAN:DSA-1018
* URL:http://www.debian.org/security/2006/dsa-1018
* FEDORA:FLSA:152532
* URL:https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=152532
* MANDRAKE:MDKSA-2005:218
* URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:218
* 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
* REDHAT:RHSA-2005:293
* URL:http://www.redhat.com/support/errata/RHSA-2005-293.html

* REDHAT:RHSA-2005:366
* URL:http://www.redhat.com/support/errata/RHSA-2005-366.html
* SUSE:SUSE-SA:2005:018
* URL:http://www.novell.com/linux/security/advisories/2005_18_kernel.html
* UBUNTU:USN-82-1
* URL:http://www.ubuntulinux.org/support/documentation/usn/usn-82-1
* SECUNIA:19374
* URL:http://secunia.com/advisories/19374
* SECUNIA:19369
* URL:http://secunia.com/advisories/19369

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2005-0449

❖ 16197 Linux Kernel error in the netfilter/iptables module can be exploited to crash the kernel

A vulnerability has been reported in the Linux kernel and can be exploited by malicious users to crash the kernel via specially crafted packets.

An error in the netfilter/iptables module can be exploited to crash the kernel via specially crafted IP packet fragments.

The vulnerability has been reported in versions 2.6 through 2.6.11.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11

Other references:
* BUGTRAQ:20050315 [USN-95-1] Linux kernel vulnerabilities
* URL:http://marc.theaimsgroup.com/?l=bugtraq&m=111091402626556&w=2
* CONECTIVA:CLA-2005:945
* URL:http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000945
* REDHAT:RHSA-2005:366
* URL:http://www.redhat.com/support/errata/RHSA-2005-366.html
* SUSE:SUSE-SA:2005:018
* URL:http://www.novell.com/linux/security/advisories/2005_18_kernel.html

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2005-0209

❖ 16198 Linux Kernel memory leak in the netfilter/iptables to be exploited to consume all available kernel memory resources

A vulnerability has been reported in the Linux kernel and can be exploited by malicious users to consume all available kernel memory resources.

A memory leak in the netfilter/iptables module when handling locally generated packet fragments can be exploited to consume all available kernel memory resources.

The vulnerability has been reported in versions 2.6 through 2.6.11.

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

Other references:
* BUGTRAQ:20050315 [USN-95-1] Linux kernel vulnerabilities
* URL:http://marc.theaimsgroup.com/?l=bugtraq&m=111091402626556&w=2
* CONECTIVA:CLA-2005:945
* URL:http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000945
* 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
* MANDRIVA:MDKSA-2005:219
* URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:219
* REDHAT:RHSA-2005:366
* URL:http://rhn.redhat.com/errata/RHSA-2005-366.html
* REDHAT:RHSA-2005:663
* URL:http://rhn.redhat.com/errata/RHSA-2005-663.html
* SUSE:SUSE-SA:2005:018
* URL:http://www.novell.com/linux/security/advisories/2005_18_kernel.html
* BID:12816
* URL:http://www.securityfocus.com/bid/12816
* OSVDB:14966
* URL:http://www.osvdb.org/14966
* SECUNIA:14295
* URL:http://secunia.com/advisories/14295
* SECUNIA:17826
* URL:http://secunia.com/advisories/17826
* SECUNIA:17002
* URL:http://secunia.com/advisories/17002

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2005-0210

❖ 16199 Linux Kernel Missing restrictions on the N_MOUSE line discipline to allow hijack another user's session

A vulnerability has been reported in the Linux kernel and can be exploited by malicious users to hijack another user's session.

Missing restrictions on the N_MOUSE line discipline makes it possible for any user to inject mouse movements and keyboard events into the input subsystem and thereby hijack another user's session.

The vulnerability has been reported in versions 2.6 through 2.6.11.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11

Other references:
* MLIST:[linux-kernel] 20050301 Re: Breakage from patch: Only root should be able to set the N_MOUSE line discipline.
* URL:http://www.mail-archive.com/linux-kernel@vger.kernel.org/msg64704.html
* MISC:http://linux.bkbits.net:8080/linux-2.6/cset@41fa6464E1UuGu6zmketEYxm73KSyQ
* FEDORA:FLSA:157459-3
* URL:http://www.securityfocus.com/archive/1/archive/1/427980/100/0/threaded
* REDHAT:RHSA-2005:366
* URL:http://www.redhat.com/support/errata/RHSA-2005-366.html

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2005-0839

New Vulnerabilities found this Week

Internet Explorer Window Loading Race Condition Address Bar Spoofing
“Conduct phishing attacks”

Hai Nam Luke has discovered a vulnerability in Internet Explorer, which can be exploited by malicious people to conduct phishing attacks.

The vulnerability is caused due to a race condition in the loading of web content and Macromedia Flash Format files (".swf") in browser windows. This can be exploited to spoof the address bar in a browser window showing web content from a malicious web site.

The vulnerability has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP1/SP2. The vulnerability has also been confirmed in Internet Explorer 7 Beta 2 Preview (March edition). Other versions may also be affected.

References:
http://secunia.com/advisories/19521/

Cisco 11500 Content Services Switch HTTP Compression Denial of Service
“Denial of Service”

A vulnerability has been reported in Cisco 11500 Content Services Switch, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the HTTP compression functionality when processing HTTP requests. This can be exploited to cause a vulnerable device to reload by sending a valid, but obsolete, or specially crafted HTTP request.

Successful exploitation requires that the network device has been configured for HTTP compression.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20060405-css.shtml

ClamAV Multiple Vulnerabilities

"Denial of Service"

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

1) An unspecified integer overflow error exists in the PE header parser in "libclamav/pe.c".

Successful exploitation requires that the ArchiveMaxFileSize option is disabled.

2) Some format string errors in the logging handling in "shared/output.c" may be exploited to execute arbitrary code.

3) An out-of-bounds memory access error in the "cli_bitset_test()" function in "ibclamav/others.c" may be exploited to cause a crash.

The vulnerabilities have been reported in version 0.88. Prior versions may also be affected.

References:
http://www.us.debian.org/security/2006/dsa-1024

Mac OS X Firmware Password Bypass Vulnerability

"Bypass the firmware password"

A vulnerability has been reported in Mac OS X, which can be exploited by malicious people with physical access to a system to bypass certain security restrictions.

The vulnerability is caused due to an unspecified error and makes it possible to bypass the firmware password and start-up an Intel-based Macintosh computer in "Single User" mode.

References:
http://docs.info.apple.com/article.html?artnum=303567

Horde Help Viewer Unspecified Code Execution Vulnerability

"Execute arbitrary code"

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

An unspecified input validation error in the help viewer can be exploited to execute arbitrary code.

The vulnerability has been reported in versions prior to 3.1.1 and 3.0.10 (from version 3.0).

References:
http://lists.horde.org/archives/announce/2006/000271.html
http://lists.horde.org/archives/announce/2006/000272.html

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