netVigilance

ScoutNews Team

January 6, 2006
2006 Issue # 1

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

EMI Virgin records [poorly] emulating SONY DRM as the consumer giant's troubles grow. Missing BlackBerry patch for 1st virus, Windows Media File zero-day exploit patch released and banks #1 hacker targets.

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

❖ Could EMI/Virgin be following in SONY's DRM footsteps?

Blogs and fan websites are lighting up over the recent discovery of DRM restrictions on the latest release from the band Coldplay; X&Y from EMI – Virgin records.

Most of the fan backlash surrounds a pamphlet included inside the CD that says the CD cannot be burned onto hard disk or another CD, converted to MP3 files, or used on an Apple computer. The protest centers on the fact that buyers are not aware of these restrictions on usage until after they purchase the CD and cannot return it.

Bloggers are calling for a boycott of Coldplay and EMI. Users feel that the record companies should make It known that DRM restrictions exist before the purchase and give the buyer the option not purchase the media.

RedHerring

Related Links :
http://www.redherring.com/Article.aspx?a=15165&hed=Coldplay+DRM+Prompts+Outcry&sector=Industries&subsector=SecurityAndDefense
http://www.bloglines.com/citations?d=1&url=http:%2F%2Fwww.boingboing.net%2F2006%2F01%2F01%2Fcoldplays_new_cd_has.html

- **SONY woes continued…**

Texas State Attorney General Greg Abbott is seeking further damages in the suit against SONY over DRM rootkit software. Atty. General Abbott stated; "We keep discovering additional methods Sony used to deceive Texas consumers who thought they were simply buying music," As a result; SONY could be liable for up to $100,000 for each violation under the Computer Spyware Act of 2005.

SC Magazine

Related Links:
http://www.oag.state.tx.us/oagnews/release.php?id=1370
http://www.scmagazine.com/us/news/article/533782/?n=us

- **BlackBerry vulnerable to tiff-bourne virus.**

The virus; transported via Tagged Image File Format (TIFF) files, could potentially disable the device's ability to open other attachments.

BlackBerry maker RIM is currently working on a patch for the flaw and does not know of any widespread infections. RIM suggested that BlackBerry users either filter TIFF files or disable their BlackBerry's attachment-opening function altogether.

CBC News

Related Links :
http://www.cbc.ca/story/business/national/2006/01/05/blackberry-060105.html?ref=rss

- **Microsoft WMF zero-day patch released**

Microsoft has released a patch for the high level vulnerability and exploit that emerged on December 27, 2005.

As reported in ScoutNews issue #52, the zero-day exploit took advantage of a hole in Windows that could permit someone to gain control of computers running Windows through .wmf files.

It is highly recommended that users immediately install this patch, see security bulletin below.

Related Links:
http://www.microsoft.com/technet/security/bulletin/ms06-001.mspx

❖ Financial institutions primary hacker target

A report published by Counterpane Internet Security claims that Financial institutions are the leading target for cyber-criminals. While Worms, Viruses and Malware still pose a financial threat in terms of downtime and resource consumption; they by no means can match the damages from data or identity theft.

Cyber crooks are more highly motivated, better funded, less risk-averse, and more tenacious than in years past and financial institutions are easy, lucrative victims.
Wall Street & Technology

Full Story :
http://www.wallstreetandtech.com/feed/showArticle.jhtml?articleID=175801626
http://www.counterpane.com/pr-20051115.html

New Vulnerabilities Tested in SecureScout

❖ 16070 Linux Kernel error in declaring the "portptr" variable to cause memory corruption 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), disclose potentially sensitive information, and bypass certain security restrictions, or by malicious people to cause a DoS.

An error in declaring the "portptr" variable that points to the port number in the conntrack tuple as static in "ip_nat_proto_tcp.c" and "ip_nat_proto_udp.c" may be exploited by malicious people to cause memory corruption by causing two packets belonging to the same protocol to be NATed at the same time.

The vulnerability has been fixed in version 2.6.13.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.13
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=d04b4f8c1c9766e49fad6a141fc61cb30db69a5c
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=fb3d89498d268c8dedc1ab5b15fa64f536564577
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=71ae18ec690953e9ba7107c7cc44589c2cc0d9f1
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=cb94c62c252796f42bb83fe40960d12f3ea5a82a
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=bfd272b1ca1164382eabaa9986aad822adb91eb2
http://www.kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.32
http://www.kernel.org/git/?p=linux/kernel/git/marcelo/linux-2.4.git;a=commit;h=e684f066dff5628bb61ad1912de6e8058b5b4c7d
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174345
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174344

Other references:
http://secunia.com/advisories/16494/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-2555, CAN-2005-2617, CAN-2005-2800, CAN-2005-3053, CVE-2005-3274, CVE-2005-3275, CVE-2005-3276, CVE-2005-3848, CVE-2005-3858

❖ 16071 Linux Kernel race condition in connection timer handling to crash the kernel 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), disclose potentially sensitive information, and bypass certain security restrictions, or by malicious people to cause a DoS.

A race condition in connection timer handling on SMP multiprocessor systems can be exploited to crash the kernel by setting up an expiration handler to modify the "ip_vs_conn_tab" connection list while the list still being traversed.

The vulnerability has been fixed in version 2.6.13.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.13

http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=d04b4f8c1c9766e49fad6a141fc61cb30db69a5c
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=fb3d89498d268c8dedc1ab5b15fa64f536564577
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=71ae18ec690953e9ba7107c7cc44589c2cc0d9f1
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=cb94c62c252796f42bb83fe40960d12f3ea5a82a
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=bfd272b1ca1164382eabaa9986aad822adb91eb2
http://www.kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.32
http://www.kernel.org/git/?p=linux/kernel/git/marcelo/linux-2.4.git;a=commit;h=e684f066dff5628bb61ad1912de6e8058b5b4c7d
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174345
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174344

Other references:
http://secunia.com/advisories/16494/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-2555, CAN-2005-2617, CAN-2005-2800, CAN-2005-3053, CVE-2005-3274, CVE-2005-3275, CVE-2005-3276, CVE-2005-3848, CVE-2005-3858

❖ 16072 Linux Kernel "sys_get_thread_area()" function to expose kernel memory 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), disclose potentially sensitive information, and bypass certain security restrictions, or by malicious people to cause a DoS.

The "sys_get_thread_area()" function does not properly clear its returned structure. This can potentially expose a small amount of kernel memory to userspace programs.

The vulnerability has been fixed in version 2.6.13.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.13
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=d04b4f8c1c9766e49fad6a141fc61cb30db69a5c
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=fb3d89498d268c8dedc1ab5b15fa64f536564577
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=71ae18ec690953e9ba7107c7cc44589c2cc0d9f1
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=cb94c62c252796f42bb83fe40960d12f3ea5a82a
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-

2.6.13.y.git;a=commit;h=bfd272b1ca1164382eabaa9986aad822adb91eb2
http://www.kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.32
http://www.kernel.org/git/?p=linux/kernel/git/marcelo/linux-2.4.git;a=commit;h=e684f066dff5628bb61ad1912de6e8058b5b4c7d
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174345
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174344

Other references:
http://secunia.com/advisories/16494/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-2555, CAN-2005-2617, CAN-2005-2800, CAN-2005-3053, CVE-2005-3274, CVE-2005-3275, CVE-2005-3276, CVE-2005-3848, CVE-2005-385

❖ 16073 Linux Kernel "icmp_push_reply function()" function to exhaust memory 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), disclose potentially sensitive information, and bypass certain security restrictions, or by malicious people to cause a DoS.

The "icmp_push_reply function()" function does not properly free memory when the "ip_append_data()" function fails. This can be exploited by malicious people to exhaust memory via a large number of specially crafted packets that cause the function to fail.

The vulnerability has been fixed in version 2.6.13.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.13
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=d04b4f8c1c9766e49fad6a141fc61cb30db69a5c
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=fb3d89498d268c8dedc1ab5b15fa64f536564577
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=71ae18ec690953e9ba7107c7cc44589c2cc0d9f1
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=cb94c62c252796f42bb83fe40960d12f3ea5a82a
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=bfd272b1ca1164382eabaa9986aad822adb91eb2
http://www.kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.32
http://www.kernel.org/git/?p=linux/kernel/git/marcelo/linux-2.4.git;a=commit;h=e684f066dff5628bb61ad1912de6e8058b5b4c7d
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174345
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174344

Other references:
http://secunia.com/advisories/16494/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-2555, CAN-2005-2617, CAN-2005-2800, CAN-2005-3053, CVE-2005-3274, CVE-2005-3275,CVE-2005-3276, CVE-2005-3848, CVE-2005-3858

❖ 16074 Linux Kernel memory leak in "ip6_input_finish()" to cause a 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), disclose potentially sensitive information, and bypass certain security restrictions, or by malicious people to cause a DoS.

A memory leak in the "ip6_input_finish()" function in "/net/ipv6/ip6_input.c" may be exploit to cause a DoS via certain malformed IPv6 packets that prevents the SKB from being freed.

The vulnerability has been fixed in version 2.6.13.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.13
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=d04b4f8c1c9766e49fad6a141fc61cb30db69a5c
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=fb3d89498d268c8dedc1ab5b15fa64f536564577
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=71ae18ec690953e9ba7107c7cc44589c2cc0d9f1
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=cb94c62c252796f42bb83fe40960d12f3ea5a82a
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=bfd272b1ca1164382eabaa9986aad822adb91eb2
http://www.kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.32
http://www.kernel.org/git/?p=linux/kernel/git/marcelo/linux-2.4.git;a=commit;h=e684f066dff5628bb61ad1912de6e8058b5b4c7d
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174345
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174344

Other references:
http://secunia.com/advisories/16494/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-2555, CAN-2005-2617, CAN-2005-2800, CAN-2005-3053, CVE-2005-3274, CVE-2005-3275, CVE-2005-3276, CVE-2005-3848, CVE-2005-3858

❖ 16075 Linux Kernel XDR Encode/Decode Buffer Overflow Vulnerability

Florian Weimer has reported a vulnerability in the Linux kernel, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the "xdr_xcode_array2()" function when encoding or decoding XDR arrays. This can be exploited to cause a buffer overflow via specially crafted XDR data for the nfsacl protocol.

The vulnerability has been fixed in version 2.6.13.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.13

Other references:
http://secunia.com/advisories/16406/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-2500

❖ 16076 Linux Kernel error within the handling of keyrings to crash the kernel 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 handling of keyrings makes it possible to crash the kernel when destroying a keyring that wasn't properly instantiated. This can be exploited by attempting to add a keyring that doesn't have an empty payload.

The vulnerability has been fixed in version 2.6.12.5.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12.5
http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=322237
http://blog.blackdown.de/2005/05/09/fixing-the-ipt_recent-netfilter-module/

Other references:
http://secunia.com/advisories/16355/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-2098, CAN-2005-2099, CAN-2005-2457, CAN-2005-2458, CAN-2005-2459, CAN-2005-2802, CAN-2005-2872

❖ 16077 Linux Kernel errors in the in-kernel zlib routines to cause 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).

Some errors in the in-kernel zlib routines can be exploited to cause a DoS via specially crafted input.

The vulnerability has been fixed in version 2.6.12.5.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12.5
http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=322237
http://blog.blackdown.de/2005/05/09/fixing-the-ipt_recent-netfilter-module/

Other references:
http://secunia.com/advisories/16355/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-2098, CAN-2005-2099, CAN-2005-2457, CAN-2005-2458, CAN-2005-2459, CAN-2005-2802, CAN-2005-2872

❖ 16078 Linux Kernel error in the driver for compressed ISO file systems to crash the kernel 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 in the driver for compressed ISO file systems can be exploited to crash the kernel when e.g. a malicious CD-ROM with a specially crafted compressed ISO image is mounted.

The vulnerability has been fixed in version 2.6.12.5.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12.5
http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=322237
http://blog.blackdown.de/2005/05/09/fixing-the-ipt_recent-netfilter-module/

Other references:
http://secunia.com/advisories/16355/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-2098, CAN-2005-2099, CAN-2005-2457, CAN-2005-2458, CAN-2005-2459, CAN-2005-2802, CAN-2005-2872

❖ 16079 Linux Kernel error in the "ipt_recent.c" netfilter module to crash kernel 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).

A array type error in the "ipt_recent.c" netfilter module when calling "memset()" on the "last_pkts" array may cause the kernel to crash via certain attacks. e.g. SSH brute force. This only affects 64-bit platforms.

The vulnerability has been fixed in version 2.6.12.5.

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
http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=322237
http://blog.blackdown.de/2005/05/09/fixing-the-ipt_recent-netfilter-module/

Other references:
http://secunia.com/advisories/16355/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-2098, CAN-2005-2099, CAN-2005-2457, CAN-2005-2458, CAN-2005-2459, CAN-2005-2802, CAN-2005-2872

New Vulnerabilities found this Week

PHP "mysql_connect" Buffer Overflow Vulnerability

“System access”

mercenary has discovered a vulnerability in PHP, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the handling of the named pipe part of the "server" parameter passed to the "mysql_connect()" PHP function in the "HANDLE create_named_pipe()" function in "libmysql.c". This can be exploited to cause a stack-based buffer overflow via a PHP script calling "mysql_connect()" where the "server" parameter can be controlled by the attacker.

NOTE: Exploit code is publicly available.

The vulnerability has been confirmed in version 4.4.1 for Windows. Versions 4.3.10 and 4.4.0 for Windows are reportedly also affected. Other versions may also be affected.

Solution:
Ensure that PHP scripts do not call the "mysql_connect()" PHP function with input originating from untrusted sources.

Provided and/or discovered by:
mercenary

Original Advisory:
http://lists.grok.org.uk/piperma...closure/2006-January/041013.html

phpDocumentor File Inclusion Vulnerabilities
“System access”

rgod has discovered two vulnerabilities in phpDocumentor, which can be exploited by malicious people to compromise a vulnerable system.

Input passed to the "FORUM[LIB]" parameter in "Documentation/tests/bug-559668.php" and the "root_dir" parameter in "docbuilder/file_dialog.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources.

Successful exploitation requires that "register_globals" is enabled.

The vulnerabilities have been confirmed in versions 1.2.3 and 1.3.0rc4 (except for the "root_dir" parameter which only has been confirmed in version 1.3.0rc4). Prior versions are reportedly also affected. Other versions may also be affected.

Solution:
Edit the source code to ensure that input is properly verified.

Set "register_globals" to "Off".

Provided and/or discovered by:
rgod

References:

http://rgod.altervista.org/phpdocumentor_130rc4_incl_expl.html

Dopewars Server Message Logging Format String Vulnerability
“DoS, system access”

A vulnerability has been reported in Dopewars, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially to compromise a vulnerable system.

The vulnerability is caused due to a format string error when writing to the log file. This can be exploited to crash the Dopewars server service and may allow arbitrary code execution.

Successful exploitation requires that the Dopewars server is run as a Windows service.

The vulnerability has been reported in versions prior to 1.5.12 and affects only the Windows version.

Solution:
Update to version 1.5.12.
http://dopewars.sourceforge.net/download.html

Note: Version 1.5.11 did not completely fix the vulnerability.

Provided and/or discovered by:
The vendor credits KF.
Original Advisory:
http://sourceforge.net/project/shownotes.php?release_id=381793

eFileGo Multiple Vulnerabilities
“DoS, Data Manipulation, System access”

dr_insane has reported some vulnerabilities in eFileGo, which can be exploited by malicious people to cause a DoS (Denial of Service), disclose sensitive information, and potentially compromise a vulnerable system.

1) An input validation error in the request handling can be exploited to browse arbitrary directories and disclose the content of arbitrary files via directory traversal attacks.

Example:
http://[host]:608/.../.../.../.../.../windows/[file]

This can further be exploited to execute arbitrary commands.

Example:
http://[host]:608/.../.../.../.../.../.../.../.../windows/system32/cmd.exe?/[command]

2) An input validation error in "upload.exe" can be exploited to consume a large amount of CPU resources on a vulnerable system by supplying an invalid upload directory.

3) An input validation error in the upload handling can be exploited to upload files to an arbitrary location via directory traversal attacks.

Example:
http://[host]:608/[directory]/cgi-bin/upload.exe?/.../.../.../.../.../.../windows/[file]

The vulnerabilities have been reported in version 3.01. Other versions may also be affected.

Solution:
Use another product.

Provided and/or discovered by:
dr_insane

Original Advisory:
http://www.ipomonis.com/advisories/PaQFile_Share.txt

phpBook "email" PHP Code Injection Vulnerability
“System access”

Aliaksandr Hartsuyeu has discovered a vulnerability in phpBook, which can be exploited by malicious people to compromise a vulnerable system.

Input passed to the "email" parameter when signing the guestbook isn't properly sanitised before being stored in a PHP script. This can be exploited to inject and execute arbitrary PHP code.

The vulnerability has been confirmed in version 1.3.2 and has also been reported in prior versions. Other versions may also be affected.

Solution:
Edit the source code to ensure that input is properly sanitised.

Use another product.

Provided and/or discovered by:
Aliaksandr Hartsuyeu

Original Advisory:
http://evuln.com/vulns/6/summary.html

AppServ "appserv_root" File Inclusion Vulnerability
“System access”

Xez has discovered a vulnerability in AppServ, which can be exploited by malicious people to compromise a vulnerable system.

Input passed to the "appserv_root" parameter in "appserv/main.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources.

The vulnerability has been confirmed in version 2.4.5. Other versions may also be affected.

Solution:
Edit the source code to ensure that input is properly verified.

Provided and/or discovered by:
Xez

NKads Login SQL Injection Vulnerability
“Security Bypass, Manipulation of data, System access”

SoulBlack Security Research has discovered a vulnerability in NKads, which can be exploited by malicious people to conduct SQL injection attacks and compromise a vulnerable system.

Input passed to the "usuario_nkads_admin" and "password_nkads_admin" parameters when logging into the administration section isn't properly sanitised before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.

Successful exploitation requires that "magic_quotes_gpc" is disabled.

This can further be exploited to bypass the authentication process and access the administration section where arbitrary PHP scripts can be uploaded to a location inside the web root (e.g. using the filename "name.jpg.php").

The vulnerability has been confirmed in version 1.0 Alfa3 (stable). Other versions may also be affected.

Solution:
Edit the source code to ensure that input is properly sanitised.

Provided and/or discovered by:
SoulBlack Security Research

Original Advisory:
http://www.soulblack.com.ar/repo/papers/advisory/nkads_advisory.txt

Juniper NetScreen Security Manager Potential Denial of Service
“DoS”

David Maciejak has reported a vulnerability in NetScreen Security Manager (NSM) which potentially can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an unspecified error in "guiSrv" and "devSrv". This can be exploited to crash the service via specially crafted input sent to port 7800 and 7801. The service reportedly will automatically be restarted by the watchdog service when it crashes.

The vulnerability has been reported in NSM 2004 FP2 and FP3. Other versions may also be affected.

Solution:
Update to version FP4r1 (2005.1).

Provided and/or discovered by:
David Maciejak

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