netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 34

August 25, 2006

Table of Contents

Product Focus

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

This Week in Review

IBM buys ISS. Look out for security issues in devices held by children. When developing software you need to know how a hacker works. 20 year old hacker faces prison.

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

- **IBM buys Internet Security Systems**

IBM and Internet Security Systems have entered into a definitive agreement for IBM to acquire Internet Security Systems in an all-cash transaction at a price of approximately $1,3 billion, or $28 per share. The acquisition is subject to Internet Security Systems shareholder and regulatory approvals and other customary closing conditions. The transaction is expected to close in the fourth quarter of 2006.

Internet Security Systems (ISS) provides security solutions to proactively protect against

Internet threats across networks, desktops and servers. ISS software, appliances and services, monitor and manage network vulnerabilities and rapidly respond in advance of potential threats.

Network Times

Full Story :
http://www.networktimes.co.za/news.aspx?pklNewsId=22193&pklIssueId=578&pklCategoryID=204

- ❖ **Hacking Wireless Networks With The PSP**

One doesn't often associate a child bearing a portable gaming console as a potential hacker, or, worse, a terrorist. We often disregard the PSP as a multimedia tool sincerely used for promoting happiness: watching movies, playing games, and listening to music.

But how about using it for infiltrating top-secret clearance level data at some of the US's most prestigous intelligence agencies? The PSP has all the prerequisites.

ITObserver

Full Story :
http://www.it-observer.com/news.php?id=6724

- ❖ **How malicious hackers attack**

When it comes to network defense, the adage "know thy enemy" is never more appropriate

When developing software or defending a network, it's helpful to understand how malicious hackers hack. A dedicated attacker will fingerprint the intended host, starting first with available IP addresses and then perform TCP -- and sometimes UDP -- scans looking for active and listening TCP/IP ports. Each found port is then further fingerprinted to determine the listening application. For example, if port 80 is found, is it running Apache or IIS?
All the applications running on the targeted host are then recorded and the underlying operating system is enumerated. At this point, the attacker has eight primary, basic ways to break in.

InfoWorld

Full Story :
http://www.infoworld.com/article/06/08/25/35OPsecadvise_1.html?source=rss&url=http://www.infoworld.com/article/06/08/25/35OPsecadvise_1.html

- ❖ **Hacker faces prison for PC attacks**

A 20-year-old California hacker who created a virus that jeopardized patients at Northwest Hospital in Seattle, damaged computers at U.S. military installations worldwide and affected thousands of others will be sentenced today. Federal prosecutors will ask U.S. District Judge Marsha Pechman to send Christopher Maxwell to prison for six years.

ITObserver

Full Story :
http://www.it-observer.com/news.php?id=6718

New Vulnerabilities Tested in SecureScout

- **16288 PHP Multiple Remote Vulnerabilities**

PHP is a software component used to dynamically generate Web pages.

PHP4 and PHP5 are reported prone to multiple remotely exploitable vulnerabilities. These issue result from insufficient sanitization of user-supplied data. A remote attacker may carry out directory traversal attacks to disclose arbitrary files and upload files to arbitrary locations.

It is reported that these vulnerabilities may only be exploited on Windows.

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

References:

Advisory:
http://www.securityfocus.com/bid/11981/

Product Page:
http://www.php.net/

CVE Reference: CAN-2004-1020

- **16289 PHP Shared Memory Module Offset Memory Corruption Vulnerability**

PHP is a software component used to dynamically generate Web pages.

PHP shared memory module (shmop) is reported prone to an integer handling vulnerability. The issue exists in the PHP_FUNCTION(shmop_write) function and is as a result of a lack of sufficient sanitization performed on 'offset' data.

This vulnerability may be exploited to make an almost arbitrary write into process memory. It is reported that the vulnerability may be leveraged to disable PHP 'safe mode', this may result in further compromise in a shared-server environment.)

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

References:

Advisory:
http://www.securityfocus.com/bid/12045/

Product Page:
http://www.php.net/

CVE Reference:

❖ 16291 PHP Mail Function ASCII Control Character Header Spoofing Vulnerability

PHP is the Personal HomePage development toolkit, distributed by the PHP.net, and maintained by the PHP Development Team in public domain.

The PHP mail function does not properly sanitize user input. Because of this, a user may pass ASCII control characters to the mail() function that could alter the headers of email. This could result in spoofed mail headers.

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

References:

Advisory:
http://www.securityfocus.com/bid/5562/

Product Page:
http://www.php.net/

CVE Reference:

❖ 16302 Vulnerabilities in Microsoft Windows Hyperlink Object Library Could Allow Remote Code Execution (MS06-050/920670) (Remote File Checking)

A remote code execution vulnerability exists in the Hyperlink Object Library. This problem exists because of an unchecked buffer in the code that is used for handling hyperlinks. An attacker could exploit the vulnerability by constructing a malicious hyperlink which could potentially lead to remote code execution if a user clicks a malicious link within an Office file or e-mail message. An attacker who successfully exploited this vulnerability could take complete control of the affected system. User interaction is required to exploit this vulnerability.

A remote code execution vulnerability exists in the Hyperlink Object Library. This problem exists when the Hyperlink Object Library uses a file containing a malformed function while handling hyperlinks. An attacker could exploit the vulnerability by constructing a malicious hyperlink which could potentially lead to remote code execution if a user clicks a malicious link within an Office file, or e-mail message. An attacker who successfully exploited this vulnerability could take complete control of the affected system. User interaction is required to exploit this vulnerability.

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

References:

Original advisory:
* MS:MS06-050
* URL:http://www.microsoft.com/technet/security/Bulletin/MS06-050.mspx

Other references:
* BUGTRAQ:20060622 MS Excel Remote Code Execution POC Exploit
* URL:http://www.securityfocus.com/archive/1/archive/1/438057/100/0/threaded
* BUGTRAQ:20060622 RE: MS Excel Remote Code Execution POC Exploit
* URL:http://www.securityfocus.com/archive/1/archive/1/438093/100/0/threaded
* BUGTRAQ:20060622 Re: MS Excel Remote Code Execution POC Exploit
* URL:http://www.securityfocus.com/archive/1/archive/1/438096/100/0/threaded
* BUGTRAQ:20060623 Re: Re: MS Excel Remote Code Execution POC Exploit
* URL:http://www.securityfocus.com/archive/1/archive/1/438156/100/0/threaded
* BUGTRAQ:20060623 Re: MS Excel Remote Code Execution POC Exploit
* URL:http://www.securityfocus.com/archive/1/archive/1/438373/100/0/threaded
* FULLDISC:20060618 ***ULTRALAME*** Microsoft Excel Unicode Overflow
* URL:http://marc.theaimsgroup.com/?l=full-disclosure&m=115067840426070&w=2
* MISC: http://www.milw0rm.com/exploits/1927
* MISC: http://blogs.technet.com/msrc/archive/2006/06/20/437826.aspx
* CERT-VN:VU#394444
* URL:http://www.kb.cert.org/vuls/id/394444
* BID:18500
* URL:http://www.securityfocus.com/bid/18500
* FRSIRT:ADV-2006-2431
* URL:http://www.frsirt.com/english/advisories/2006/2431
* OSVDB:26666
* URL:http://www.osvdb.org/26666
* SECTRACK:1016339
* URL:http://securitytracker.com/id?1016339
* SECUNIA:20748
* URL:http://secunia.com/advisories/20748
* CERT:TA06-220A
* URL:http://www.us-cert.gov/cas/techalerts/TA06-220A.html
* CERT-VN:VU#683612
* URL:http://www.kb.cert.org/vuls/id/683612

CVE Reference: CVE-2006-3086

❖ 16303 Vulnerability in Windows Kernel Could Result in Remote Code Execution (MS06-051/917422) (Remote File Checking)

There is a privilege elevation vulnerability in the way that Windows 2000 starts applications. This vulnerability could allow a logged on user to take complete control of the system.

There is a remote code execution vulnerability in the way that exception handling is managed on multiple applications that are resident in memory.

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

References:

Original advisory:
* MS:MS06-051
* URL:http://www.microsoft.com/technet/security/Bulletin/MS06-051.mspx

Other references:
* BID:19375
* URL:http://www.securityfocus.com/bid/19375
* FRSIRT:ADV-2006-3216
* URL:http://www.frsirt.com/english/advisories/2006/3216
* SECUNIA:21417
* URL:http://secunia.com/advisories/21417
* CERT:TA06-220A
* URL:http://www.us-cert.gov/cas/techalerts/TA06-220A.html
* CERT-VN:VU#411516
* URL:http://www.kb.cert.org/vuls/id/411516
* URL:http://www.frsirt.com/english/advisories/2006/3216

CVE Reference: CVE-2006-3443

❖ 16304 PHP "sscanf()" Code Execution Safe Mode Bypass Vulnerability

PHP is the Personal HomePage development toolkit, distributed by the PHP.net, and maintained by the PHP Development Team in public domain.

Heintz has discovered a vulnerability in PHP, which potentially can be exploited by malicious, local users to bypass certain security restrictions.

The vulnerability is caused due to an array boundary error in the "sscanf()" PHP function in the processing of the "%1s" format specifier. This can be exploited to reference freed memory by passing an variable as argument which has been unset.

Successful exploitation may e.g. allow bypass of the safe mode protection by executing arbitrary code.

The vulnerability has been confirmed in versions 5.1.4 and 4.4.3. Other versions may also be affected.

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

References:

Original Advisory:
http://bugs.php.net/bug.php?id=38322

Other references:
BUGTRAQ:20060804 php local buffer underflow could lead to arbitary code execution
URL:http://www.securityfocus.com/archive/1/442438/30/0/threaded
MISC: http://www.plain-text.info/sscanf_bug.txt
CONFIRM: http://bugs.php.net/bug.php?id=38322

BID:19415
URL:http://www.securityfocus.com/bid/19415
FRSIRT:ADV-2006-3193
URL:http://www.frsirt.com/english/advisories/2006/3193
SECUNIA:21403
URL:http://secunia.com/advisories/21403

Product Page:
http://www.php.net/

CVE Reference: CVE-2006-4020

❖ 16305 PHP "error_log()" Safe Mode Bypass Vulnerability

PHP is the Personal HomePage development toolkit, distributed by the PHP.net, and maintained by the PHP Development Team in public domain.

Maksymilian Arciemowicz has discovered a weakness in PHP, which can be exploited by malicious, local users to bypass certain security restrictions.

The weakness is caused due to an input validation error in the "error_log()" PHP function in the processing of the destination parameter. This can be exploited to bypass the safe mode protection via directory traversal attacks in the "php://" wrapper.

The weakness has been confirmed in version 5.1.4 and has also been reported in version 4.4.2. Other versions may also be affected.

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

References:

Original Advisory:
http://securityreason.com/achievement_securityalert/41

Other references:
BUGTRAQ:20060625 error_log() Safe Mode Bypass PHP 5.1.4 and 4.4.2
URL:http://www.securityfocus.com/archive/1/archive/1/438436/100/0/threaded
MISC: http://securityreason.com/achievement_securityalert/41
MANDRIVA:MDKSA-2006:122
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:122
CONFIRM: http://cvs.php.net/viewvc.cgi/php-src/ext/standard/basic_functions.c?r1=1.543.2.51.2.9&r2=1.543.2.51.2.10&pathrev=PHP_4_4&diff_format=u
CONFIRM: http://cvs.php.net/viewvc.cgi/php-src/ext/standard/basic_functions.c?diff_format=u&view=log&pathrev=PHP_4_4
UBUNTU:USN-320-1
URL:http://www.ubuntu.com/usn/usn-320-1
FRSIRT:ADV-2006-2523
URL:http://www.frsirt.com/english/advisories/2006/2523
OSVDB:26827
URL:http://www.osvdb.org/26827
SECTRACK:1016377
URL:http://securitytracker.com/id?1016377

SECUNIA:20818
URL:http://secunia.com/advisories/20818
SECUNIA:21050
URL:http://secunia.com/advisories/21050
XF:php-errorlog-safe-mode-bypass(27414)
URL:http://xforce.iss.net/xforce/xfdb/27414

Product Page:
http://www.php.net/

CVE Reference: CVE-2006-3011

❖ 16306 PHP "substr_compare()" offset/length parameter validation error Vulnerability

PHP is the Personal HomePage development toolkit, distributed by the PHP.net, and maintained by the PHP Development Team in public domain.

A vulnerability has been reported in PHP that can be exploited by malicious people to bypass certain security restrictions.

An offset/length parameter validation error exists in the "substr_compare()" function.

The issue has been fixed in PHP version 4.4.3.

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

References:

Original Advisory:
http://www.php.net/release_4_4_3.php

Other references:
MANDRIVA:MDKSA-2006:122
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:122
UBUNTU:USN-320-1
URL:http://www.ubuntu.com/usn/usn-320-1
OSVDB:25253
URL:http://www.osvdb.org/25253
SECTRACK:1016306
URL:http://securitytracker.com/id?1016306
SECUNIA:19927
URL:http://secunia.com/advisories/19927
SECUNIA:21050
URL:http://secunia.com/advisories/21050

Product Page:
http://www.php.net/

CVE Reference: CVE-2006-3016

❖ 16307 PHP session name character handling Vulnerability

PHP is the Personal HomePage development toolkit, distributed by the PHP.net, and maintained by the PHP Development Team in public domain.

A vulnerability has been reported in PHP that can be exploited by malicious people to bypass certain security restrictions.

An unspecified error exists in the handling of certain characters in session names.

The issue has been fixed in PHP version 4.4.3.

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

References:

Original Advisory:
http://www.php.net/release_4_4_3.php

Other references:
MANDRIVA:MDKSA-2006:122
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:122
UBUNTU:USN-320-1
URL:http://www.ubuntu.com/usn/usn-320-1
OSVDB:25253
URL:http://www.osvdb.org/25253
SECTRACK:1016306
URL:http://securitytracker.com/id?1016306
SECUNIA:19927
URL:http://secunia.com/advisories/19927
SECUNIA:21050
URL:http://secunia.com/advisories/21050

Product Page:
http://www.php.net/

CVE Reference: CVE-2006-3016

❖ 16308 PHP "unset()" to not unset variables properly Vulnerability

PHP is the Personal HomePage development toolkit, distributed by the PHP.net, and maintained by the PHP Development Team in public domain.

A vulnerability has been reported in PHP that can be exploited by malicious people to bypass certain security restrictions.

An error in the "zend_hash_del_key_or_index()" function when deleting elements can e.g. be exploited to cause the "unset()" function to not unset variables properly.

The issue has been fixed in PHP version 4.4.3.

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

References:

Original Advisory:
http://www.php.net/release_4_4_3.php

Other references:
MANDRIVA:MDKSA-2006:122
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:122
UBUNTU:USN-320-1
URL:http://www.ubuntu.com/usn/usn-320-1
OSVDB:25253
URL:http://www.osvdb.org/25253
SECTRACK:1016306
URL:http://securitytracker.com/id?1016306
SECUNIA:19927
URL:http://secunia.com/advisories/19927
SECUNIA:21050
URL:http://secunia.com/advisories/21050

Product Page:
http://www.php.net/

CVE Reference: CVE-2006-3016

New Vulnerabilities found this Week

Internet Explorer URL Compression Buffer Overflow Vulnerability

"System access"

A vulnerability has been reported in Internet Explorer, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the "CMimeFt::Start()" function within urlmon.dll when processing URLs on a website using HTTP 1.1 and compression. This can be exploited to cause a heap-based buffer overflow via an overly long URL (more than 260 bytes).

Successful exploitation allows execution of arbitrary code when a user is e.g. tricked into visiting a malicious website.

The vulnerability affects Internet Explorer 6 SP1 on Windows 2000 and Windows XP SP1 and was introduced by the MS06-042 patches.

References:

Original Advisory:
MS06-042 (KB918899):
http://www.microsoft.com/china/technet/security/bulletin/MS06-042.mspx

Microsoft:
http://www.microsoft.com/technet/security/advisory/923762.mspx
http://support.microsoft.com/kb/923762/
http://blogs.technet.com/msrc/archive/2006/08/24/449860.aspx

eEye Digital Security:
http://research.eeye.com/html/advisories/published/AD20060824.html

NSFocus Security Team:
http://www.nsfocus.com/english/homepage/research/0608.htm

Other References:
US-CERT VU#821156:
http://www.kb.cert.org/vuls/id/821156

PHP Multiple Vulnerabilities
"Security Bypass"

Some vulnerabilities have been reported in PHP, where some have unknown impacts, and others can be exploited by malicious, local users to bypass certain security restrictions.

1) Missing safe_mode and open_basedir verification exists in the "file_exists()", "imap_open()", and "imap_reopen()" functions.

2) Some unspecified boundary errors exists in the "str_repeat()" and "wordwrap()" functions on 64-bit systems.

3) The open_basedir and safe_mode protection mechanisms can be bypassed via the cURL extension and the realpath cache.

4) An unspecified boundary error exists in the GD extension when handling malformed GIF images.

5) A boundary error in the "stripos()" function can be exploited to cause an out-of-bounds memory read.

6) Incorrect memory_limit restrictions exists on 64-bit systems.

Other issues which may be security related have also been reported.

References:

Original Advisory:
http://www.php.net/release_4_4_4.php
http://www.php.net/release_5_1_5.php

Ichitaro Document Viewer Buffer Overflow Vulnerability
"System access"

A vulnerability has been reported in Ichitaro, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error when processing a specially crafted document. This can be exploited to cause a stack-based buffer overflow via an overly long string.

Successful exploitation allows execution of arbitrary code.

NOTE: The vulnerability is currently being actively exploited.

References:

Original Advisory:
Justsystem (japanese):
http://www.justsystem.co.jp/info/pd6002.html

PowerZip File Handling Buffer Overflow Vulnerability
"System access"

Tan Chew Keong has reported a vulnerability in PowerZip, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the handling of filenames in ZIP archives. This can be exploited to cause a stack-based buffer overflow when a malicious ZIP archive containing a file with an overly long filename is opened.

Successful exploitation allows execution of arbitrary code.

The vulnerability has been reported in version 7.06 Build 3895. Prior versions may also be affected.

References:

Original Advisory:
http://vuln.sg/powerzip706-en.html

Symantec Enterprise Security Manager Denial of Service
"Denial of Service"

A vulnerability has been reported in Symantec Enterprise Security Manager (ESM), which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to a race condition when processing certain requests. This can be exploited by sending a specially crafted, invalid request to the manager service to simulate an ESM agent.

Successful exploitation causes both the ESM agent and ESM manager to stop responding.

The vulnerability has been reported in versions 6.0 through 6.5.x. Prior versions may also be affected.

References:

Original Advisory:
Symantec:
http://securityresponse.symantec.com/avcenter/security/Content/2006.08.21a.html
http://securityresponse.symantec.com/avcenter/security/Content/2006.08.21c.html

WebAdmin Account Manipulation and Arbitrary File Disclosure
"Exposure of sensitive information"

TTG has reported some vulnerabilities in WebAdmin, which can be exploited by certain malicious users to manipulate or gain knowledge of sensitive information.

1) Input passed to the "file" parameter in logfile_view.wdm and configfile_view.wdm is not properly sanitised before being used to show files. This can be exploited by a global administrative user to view the contents of arbitrary files via directory traversal attacks.

2) It possible for a domain administrative user to edit a global administrative user's account. This can be exploited to change the password and then login as the global administrative user.

References:

http://secunia.com/advisories/21558/

Horde IMP Folder Names Script Insertion Vulnerability
"Cross Site Scripting"

Marc Ruef has reported a vulnerability in Horde IMP, which can be exploited by malicious users to conduct script insertion attacks.

Input passed to the folder names isn't properly sanitised before being used. This can be exploited to inject arbitrary HTML and script code, which will be executed in a user's browser session in context of an affected site when the malicious user data is viewed via a shared folder.

The vulnerability has been reported in versions 4.0.4 and 4.1.2. Prior versions may also be affected.

References:

Original Advisory:
http://lists.horde.org/archives/announce/2006/000293.html
http://lists.horde.org/archives/announce/2006/000294.html

Mambo Coppermine Component File Inclusion Vulnerability
“System access”

k1tk4t has discovered a vulnerability in the Coppermine component for Mambo, which can be exploited by malicious people to compromise a vulnerable system.

Input passed to the "mosConfig_absolute_path" parameter in components/com_cpg/cpg.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 vulnerability has been confirmed in version 1.0. Other versions may also be affected.

References:

Original Advisory:
http://milw0rm.com/exploits/2196

Mambo mosListMessenger Component File Inclusion
"System access"

Crackers_Child has reported a vulnerability in the mosListMessenger component for Mambo, which can be exploited by malicious people to compromise a vulnerable system.

Input passed to the "mosConfig_absolute_path" parameter in components/com_lm/archive.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.

References:

http://secunia.com/advisories/21531/

IBM eGatherer ActiveX "RunEgatherer" Buffer Overflow
"System access"

eEye Digital Security has reported a vulnerability in the IBM eGatherer ActiveX control, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error within the RunEgatherer function and can be exploited to cause a stack-based overflow by e.g. tricking a user into visiting a malicious website.

Successful exploitation allows execution of arbitrary code.

References:

Original Advisory:
http://www.eeye.com/html/research/advisories/AD20060816.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