netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 47

November 30, 2007

Table of Contents

Product Focus

This Week in Review

Top Security News Stories this Week

New Vulnerabilities Tested in SecureScout

New Vulnerabilities found this Week

Product Focus

Sapphire Worm Scanner – The Sapphire Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the Microsoft SQL buffer overflow vulnerability (MS02-039/MS02-061) that the recent Sapphire Worm uses to propagate.

This Week in Review

Companies have a false sense of being secure. Botnet cracked by FBI. Each year data breaches are more costly. Our own Jesper Jurcenoks on choosing security consultants.

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

- **Majority companies feel they are secure against the risk of data leaks**

The email survey, conducted during the week of the HMRC data loss, showed that the majority of respondents feel their companies are secure against the risk of data leaks. Just 11% of respondents said that HMRC's highly-publicised loss of CDs, containing personal details of 25M UK citizens, would influence their IT spending priorities.

However, the survey revealed that the organisations surveyed are still running the risk of data loss similar to HMRC. Less than half of respondents (48%) said their organisation had an encryption solution to protect sensitive data. 40% of the sample said their company did not have encryption, and a worrying 12% did not know if encryption was in place.

Help net security

Full Story :
http://www.net-security.org/secworld.php?id=5640

❖ FBI crackdown on botnets gets results, but damage continues

FBI agents engaged in a crackdown on botnet crime issued a progress report of the ongoing initiative, reporting more than $20m in losses to consumers, businesses and other organizations and the identification of one million infected machines in the past five months.

In addition, eight individuals have been indicted, have pleaded guilty or been sentenced for crimes related to botnets since "Operation Bot Roast," as the ongoing investigation is known, was announced in June. Thirteen search warrants connected to the operation have been served in the US and overseas, and at least seven FBI field offices have participated.

Combined with the FBI's previous tally, federal investigators have now identified more than two million zombie computers, so called because they mindlessly follow the orders of their devious masters.

The Register

Full Story :
http://www.theregister.co.uk/2007/11/29/fbi_botnet_progress_report/

❖ Study: Cost of Data Breaches Rising

Dr. Larry Ponemon, chairman and founder of the Ponemon Institute, said in a statement announcing the results of the Ponemon Institute's study on data breaches that, although companies are responding to data breaches more efficiently, consumers seem to be less forgiving when their personal information is compromised.
According to a study released on Thursday by the Ponemon Institute, a privacy and information management research firm, each customer record lost or compromised in 2007 cost companies $197, compared to $182 in 2006. That represents an increase of more than 8 percent.

This is the third year that the Ponemon Institute has conducted its "U.S. Cost of a Data Breach" survey; the average per-incident cost has climbed each year. The increase between 2005 and 2006 was particularly steep, clocking in at over 40 percent.

CIO TODAY

Full Story :

http://www.cio-today.com/news/Study--Cost-of-Data-Breaches-Rising/story.xhtml?story_id=132004JUOKPO

- **Surprising advice on picking a good security consultant**

During the ITEC MasterMinds Security Panel in Philadelphia, an attendee asked a great question. "Since I give these people the keys to my entire business, how do I pick a good security consultant?"
Luckily, David Troup of MailFoundry (.com) and Jesper Jurcenoks of NetVigilance (.com) were on the panel and gave excellent advice. Some details I expected, but one caught me by surprise.

* Certifications from applicable vendors, mainly Cisco, lead the conversation. If your primary vendor offers certifications, you'd look for those first, but few vendors offer specialized security training. Hence, Cisco becomes the ticket of choice.

ITworld

Full Story :
http://www.itworld.com/Net/nlsnetwork071127/

New Vulnerabilities Tested in SecureScout

- **17773 PHP deserialization of session data, arbitrary code execution Vulnerability**

PHP, when register_globals is enabled, allows context-dependent attackers to execute arbitrary code via deserialization of session data, which overwrites arbitrary global variables, as demonstrated by calling session_decode on a string beginning with "_SESSION|s:39:".

The vulnerability has been confirmed in version 4 lower than 4.4.5 and 5

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

References:

* MISC:
http://www.php-security.org/MOPB/MOPB-31-2007.html
* GENTOO: GLSA-200705-19
http://security.gentoo.org/glsa/glsa-200705-19.xml
* HP: HPSBMA02215
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?lang=en&cc=us&objectID=c01056506
* HP: HPSBTU02232
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?lang=en&cc=us&objectID=c01086137
* BID: 23120
http://www.securityfocus.com/bid/23120
* FRSIRT: ADV-2007-1991
http://www.frsirt.com/english/advisories/2007/1991
* FRSIRT: ADV-2007-2374

http://www.frsirt.com/english/advisories/2007/2374
* SECUNIA: 25445
http://secunia.com/advisories/25445
* SECUNIA: 25423
http://secunia.com/advisories/25423
* SECUNIA: 25850
http://secunia.com/advisories/25850

CVE Reference: CVE-2007-1701

❖ 17772 PHP session extension, arbitrary code execution Vulnerability

The session extension in PHP, calculates the reference count for the session variables without considering the internal pointer from the session globals, which allows context-dependent attackers to execute arbitrary code via a crafted string in the session_register after unsetting HTTP_SESSION_VARS and _SESSION, which destroys the session data Hashtable.

The vulnerability has been confirmed in version 4 lower than 4.4.5 and 5 lower than 5.2.1.

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

References:

* MISC:
http://www.php-security.org/MOPB/MOPB-30-2007.html
* DEBIAN: DSA-1283
http://www.debian.org/security/2007/dsa-1283
* GENTOO: GLSA-200705-19
http://security.gentoo.org/glsa/glsa-200705-19.xml
* HP: HPSBMA02215
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?lang=en&cc=us&objectID=c01056506
* HP: HPSBTU02232
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?lang=en&cc=us&objectID=c01086137
* SUSE: SUSE-SA:2007:032
http://www.novell.com/linux/security/advisories/2007_32_php.html
* UBUNTU: USN-455-1
http://www.ubuntu.com/usn/usn-455-1
* BID: 23119
http://www.securityfocus.com/bid/23119
* FRSIRT: ADV-2007-1991
http://www.frsirt.com/english/advisories/2007/1991
* FRSIRT: ADV-2007-2374
http://www.frsirt.com/english/advisories/2007/2374
* SECUNIA: 25062
http://secunia.com/advisories/25062
* SECUNIA: 25057
http://secunia.com/advisories/25057
* SECUNIA: 25056

http://secunia.com/advisories/25056
* SECUNIA: 25445
http://secunia.com/advisories/25445
* SECUNIA: 25423
http://secunia.com/advisories/25423
* SECUNIA: 25850
http://secunia.com/advisories/25850

CVE Reference: CVE-2007-1700

❖ 17771 PHP zend_hash_init function, denial of service Vulnerability

The zend_hash_init function in PHP, when running on a 64-bit platform, allows context-dependent attackers to cause a denial of service (infinite loop) by unserializing certain integer expressions, which only cause 32-bit arguments to be used after the check for a negative value, as demonstrated by an "a:2147483649:{" argument.

The vulnerability is confirmed in version 5.2.0 and also reported in version 4.4.4. Other versions may also be affected.

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

Some References:

* BUGTRAQ: 20070227 rPSA-2007-0043-1 php php-mysql php-pgsql
http://www.securityfocus.com/archive/1/archive/1/461462/100/0/threaded
* MISC:
http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=228858
* MISC:
http://www.php.net/releases/5_2_1.php
* MISC:
http://www.php-security.org/MOPB/MOPB-05-2007.html
* CONFIRM:
https://issues.rpath.com/browse/RPL-1088
* CONFIRM:
http://support.avaya.com/elmodocs2/security/ASA-2007-101.htm
* CONFIRM:
http://support.avaya.com/elmodocs2/security/ASA-2007-136.htm
* DEBIAN: DSA-1264
http://www.us.debian.org/security/2007/dsa-1264
* GENTOO: GLSA-200703-21
http://security.gentoo.org/glsa/glsa-200703-21.xml
* HP: HPSBMA02215
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?lang=en&cc=us&objectID=c01056506

CVE Reference: CVE-2007-0988

❖ 17770 PHP Integer overflow in the msg_receive function Vulnerability

Integer overflow in the msg_receive function in PHP, on FreeBSD and possibly other platforms, allows context-dependent attackers to execute arbitrary code via certain maxsize values, as demonstrated by 0xffffffff.

The vulnerability is confirmed in version 5.2.0 and also reported in version 4.4.4. Other versions may also be affected.

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

References:

* MISC:
http://www.php-security.org/MOPB/MOPB-43-2007.html
* BID: 23236
http://www.securityfocus.com/bid/23236

CVE Reference: CVE-2007-1890

❖ 17769 PHP Integer signedness error in the _zend_mm_alloc_int function Vulnerability

Integer signedness error in the _zend_mm_alloc_int function in the Zend Memory Manager in PHP allows remote attackers to execute arbitrary code via a large emalloc request, related to an incorrect signed long cast, as demonstrated via the HTTP SOAP client in PHP, and via a call to msg_receive with the largest positive integer value of maxsize.

The vulnerability is confirmed in version 5.2.0.

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

References:

* MISC:
http://www.php-security.org/MOPB/MOPB-44-2007.html
* DEBIAN: DSA-1283
http://www.debian.org/security/2007/dsa-1283
* SUSE: SUSE-SA:2007:032
http://www.novell.com/linux/security/advisories/2007_32_php.html
* SECUNIA: 25062
http://secunia.com/advisories/25062
* SECUNIA: 25056
http://secunia.com/advisories/25056

CVE Reference: CVE-2007-1889

❖ 17768 PHP Buffer overflow in the sqlite_decode_binary function in src/encode.c in SQLite 2 Vulnerability

Buffer overflow in the sqlite_decode_binary function in src/encode.c in SQLite 2, as used by PHP and other applications, allows context-dependent attackers to execute arbitrary code via an empty value of the in parameter.

The vulnerability is confirmed in version 5.2.0 and also reported in version 4.4.4. Other versions may also be affected.

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

Some References:

* MISC:
http://www.php-security.org/MOPB/MOPB-41-2007.html
* MISC:
http://www.sqlite.org/cvstrac/rlog?f=sqlite/src/encode.c
* MANDRIVA: MDKSA-2007:091
http://www.mandriva.com/security/advisories?name=MDKSA-2007:091
* UBUNTU: USN-455-1
http://www.ubuntu.com/usn/usn-455-1
* VIM: 20070422 vendor ack/clarification for CVE-2007-1888 (SQLite)
http://www.attrition.org/pipermail/vim/2007-April/001540.html
* SECUNIA: 25057
http://secunia.com/advisories/25057

CVE Reference: CVE-2007-1888

❖ 17767 PHP sqlite_decode_binary function, Buffer overflow Vulnerability

Buffer overflow in the sqlite_decode_binary function in the bundled sqlite library in PHP allows context-dependent attackers to execute arbitrary code via an empty value of the in parameter, as demonstrated by calling the sqlite_udf_decode_binary function with a 0x01 character.

The vulnerability is confirmed in version 5.2.0 and also reported in version 4.4.4. Other versions may also be affected.

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

References:

* MISC:
http://www.php-security.org/MOPB/MOPB-41-2007.html
* CONFIRM:
http://www.php.net/releases/5_2_1.php
* CONFIRM:
http://www.php.net/releases/5_2_3.php
* DEBIAN: DSA-1283
http://www.debian.org/security/2007/dsa-1283
* FEDORA: FEDORA-2007-2215
https://www.redhat.com/archives/fedora-package-announce/2007-September/msg00397.html
* HP: HPSBUX02262
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c0

1178795
* MANDRIVA: MDKSA-2007:088
http://www.mandriva.com/security/advisories?name=MDKSA-2007:088
* MANDRIVA: MDKSA-2007:089
http://www.mandriva.com/security/advisories?name=MDKSA-2007:089
* UBUNTU: USN-455-1
http://www.ubuntu.com/usn/usn-455-1
* BID: 23235
http://www.securityfocus.com/bid/23235
* FRSIRT: ADV-2007-2016
http://www.frsirt.com/english/advisories/2007/2016
* FRSIRT: ADV-2007-3386
http://www.frsirt.com/english/advisories/2007/3386
* SECUNIA: 25062
http://secunia.com/advisories/25062
* SECUNIA: 25057
http://secunia.com/advisories/25057
* SECUNIA: 24909
http://secunia.com/advisories/24909
* SECUNIA: 27037
http://secunia.com/advisories/27037
* SECUNIA: 27110
http://secunia.com/advisories/27110

CVE Reference: CVE-2007-1887

❖ 17766 PHP printf function family, Multiple integer signedness errors Vulnerability

Multiple integer signedness errors in the printf function family in PHP on 64 bit machines allow context-dependent attackers to execute arbitrary code via (1) certain negative argument numbers that arise in the php_formatted_print function because of 64 to 32 bit truncation, and bypass a check for the maximum allowable value; and (2) a width and precision of -1, which make it possible for the php_sprintf_appendstring function to place an internal buffer at an arbitrary memory location.

The vulnerability is confirmed in version 5.2.0 and also reported in version 4.4.4. Other versions may also be affected.

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

References:

* MISC:
http://www.php-security.org/MOPB/MOPB-38-2007.html
* CONFIRM:
http://www.php.net/releases/5_2_1.php
* HP: HPSBMA02215
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?lang=en&cc=us&objectID=c01056506
* HP: HPSBTU02232
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?lang=en&cc=us&objectID=c01086137

* BID: 23219
http://www.securityfocus.com/bid/23219
* FRSIRT: ADV-2007-1991
http://www.frsirt.com/english/advisories/2007/1991
* FRSIRT: ADV-2007-2374
http://www.frsirt.com/english/advisories/2007/2374
* OSVDB: 33955
http://www.osvdb.org/33955
* OSVDB: 34767
http://www.osvdb.org/34767
* SECUNIA: 25423
http://secunia.com/advisories/25423
* SECUNIA: 25850
http://secunia.com/advisories/25850

CVE Reference: CVE-2007-1884

❖ 17765 PHP FDF support (ext/fdf), input filtering hooks missing Vulnerability

The FDF support (ext/fdf) in PHP does not implement the input filtering hooks for ext/filter, which allows remote attackers to bypass web site filters via an application/vnd.fdf formatted POST.

The vulnerability is confirmed in version 5.x < 5.2.0.

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

References:

* MISC:
http://www.php-security.org/MOPB/MOPB-17-2007.html
* BID: 22906
http://www.securityfocus.com/bid/22906

CVE Reference: CVE-2007-1452

❖ 17764 PHP variable reference counter, Integer overflow Vulnerability

Integer overflow in the 16 bit variable reference counter in PHP 4 allows context-dependent attackers to execute arbitrary code by overflowing this counter, which causes the same variable to be destroyed twice.

The vulnerability is confirmed in 4.x up to 4.4.4.

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

References:

* MISC:
http://www.php-security.org/MOPB/MOPB-01-2007.html

* GENTOO: GLSA-200703-21
http://security.gentoo.org/glsa/glsa-200703-21.xml
* SUSE: SUSE-SA:2007:032
http://www.novell.com/linux/security/advisories/2007_32_php.html
* BID: 22765
http://www.securityfocus.com/bid/22765
* OSVDB: 32770
http://www.osvdb.org/32770
* SECUNIA: 24606
http://secunia.com/advisories/24606
* SECUNIA: 25056
http://secunia.com/advisories/25056

CVE Reference: CVE-2007-1383

New Vulnerabilities found this Week

Apple QuickTime RTSP "Content-Type" Header Buffer Overflow
"Execution of arbitrary code"

h07 has discovered a vulnerability in Apple QuickTime, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error when processing RTSP replies and can be exploited to cause a stack-based buffer overflow via a specially crafted RTSP reply containing an overly long "Content-Type" header.

Successful exploitation allows execution of arbitrary code and requires that the user is e.g. tricked into opening a malicious QTL file or visiting a malicious web site.

The vulnerability is confirmed in version 7.3. Other versions may also be affected.

References:
http://www.milw0rm.com/exploits/4648

IBM Lotus Notes Lotus 1-2-3 File Viewer Buffer Overflows
"Execution of arbitrary code"

Some vulnerabilities have been reported in IBM Lotus Notes, which can be exploited by malicious people to compromise a user's system.

The vulnerabilities are caused due to boundary errors within the Lotus 1-2-3 file viewer (l123sr.dll) and can be exploited to cause buffer overflows by tricking a user into viewing a specially crafted Lotus 1-2-3 attachment with e.g. a specially crafted type SRANGE record.

Successful exploitation allows execution of arbitrary code.

The vulnerabilities reportedly affect versions 7.0 and 8.0.

References:
http://www-1.ibm.com/support/docview.wss?uid=swg21285600

Symantec Backup Exec Job Engine Denial of Service Vulnerabilities
"Denial of Service"

Secunia Research has discovered some vulnerabilities in Symantec Backup Exec for Windows Servers, which can be exploited by malicious people to cause a DoS (Denial of Service).

1) A NULL-pointer dereference error in the Backup Exec Job Engine service (bengine.exe) when handling exceptions can be exploited to crash the service by sending a specially crafted packet to default port 5633/TCP.

2) Two integer overflow errors within the Backup Exec Job Engine service can be exploited to e.g. cause the service to enter an infinite loop and exhaust all available memory or consume large amounts of CPU resource by sending a specially crafted packet to default port 5633/TCP.

The vulnerabilities are confirmed in Symantec Backup Exec for Windows Servers version 11d build 11.0.7170 and also affect version 11d build 11.0.6.6235.

References:
http://securityresponse.symantec.com/avcenter/security/Content/2007.11.27.html

FTP Admin Multiple Vulnerabilities
"Cross-site scripting attacks; Bypass security restrictions"

Omni has discovered some vulnerabilities in FTP Admin, which can be exploited by malicious users to compromise a vulnerable system, and by malicious people to conduct cross-site scripting attacks and bypass certain security restrictions.

1) Input passed to the "page" parameter in index.php is not properly verified before being used to include files. This can be exploited to include arbitrary files from local resources or external FTP resources.

Successful exploitation of this vulnerability requires valid user credentials (but see #2).

2) A vulnerability is caused due to improper authentication verification in index.php. This can be exploited to log in and e.g. add new FTP users without having valid user credentials, by setting the "loggedin" parameter to "true".

Successful exploitation of this vulnerability requires that "register_globals" is enabled.

3) Input passed to the "error" parameter in index.php (when "page" is set to "error") is not properly sanitised before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

The vulnerabilities are confirmed in version 0.1.0. Other versions may also be affected.

References:
http://milw0rm.com/exploits/4681

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