netVigilance
assurance has arrived

2007 Issue # 35

ScoutNews

The weekly Security update from the makers of SecureScout

September 7, 2007

Table of Contents

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

PCI Security Standards a step on the way. How to secure your database. London is the UK's capital for online credit card fraud. A "hardened" set of security guidelines for VMware's ESX Server on its way.

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

- **Vendor report: PCI; Is your Business up to the Standard?**

With security breaches causing more high-profile harm to corporations and their customers than ever, companies today face intense scrutiny as to how well they secure the privacy and integrity of account information and other confidential files. Incidents, like the hacker attack on the central database of retailer TJX resulted in the theft of credit and debit card information of nearly 50 million customers, are driving government and industry regulators to step up compliance requirements.

Companies are feeling the heat, with security professionals consistently ranking policy and regulatory compliance at or near the top of their priority lists - dedicating more time and money to meeting security mandates. This pressure is unlikely to abate any time soon, with influential industry groups, such as the Payment Card Industry, (PCI) increasing their requirements in specifications such as the 12–point best practice areas outlined in its PCI Data Security Standard (DSS). PCI DSS requires businesses be audited annually by an outside firm. And as states such as Texas weigh the adoption of PCI standards as law, companies may come under real legal fire to meet these specifications.

computerweekly

Full Story :
http://www.computerweekly.com/Articles/2007/09/06/226599/vendor-report-pci-is-your-business-up-to-the-standard.htm

❖ Database Security in 5 Steps

Forrester Research analyst Noel Yuhanna stresses that enterprises need a database security plan.
ATLANTA - Monster.com, TJX, Pfizer—the list of companies and organizations affected by database breaches grows bigger and badder every week, but most enterprises remain focused on the perimeter and ignore the database.
Some 80 percent of enterprises lack a basic database security plan, according to Forrester Research surveys.

"People take it for granted that databases are secure," said Noel Yuhanna, a principal analyst at Forrester Research, in Cambridge, Mass. "You can't buy a product, and that's it, it's secure. A lot of people don't even have a database security plan."

eweek

Full Story :
http://www.eweek.com/article2/0,1759,2179599,00.asp

❖ London is UK's online fraud hotspot

London is the UK's capital for online credit card fraud, according to a recent report which maps the UK's card fraud hotspots.

The latest figures from Early Warning for cardholder not present (CNP) fraud show that Greater London had the largest number of fraudulent transactions in the past year, followed by Manchester and Kilmarnock.

Early Warning helps retailers, the police and banks monitor and counter online credit card fraud.

The company produces a map that identifies the postcode areas from which the fraudsters operate by tracking the delivery addresses for fraudulently obtained goods, typically accommodation addresses and 'dead' letter boxes.

vnunet

Full Story :
http://www.vnunet.com/vnunet/news/2198214/london-uk-online-fraud-hotspot

❖ Finally, A Way To Measure Real Security On A Virtual Machine

The Center for Internet Security will be floating an early version of a "hardened" set of security guidelines for VMware's ESX Server.
The upcoming VMworld conference will feature, in addition to a raft of new products, the the draft of a guide on how to make virtual machines more secure, addressing one of the most sensitive issues in the burgeoning adoption of virtualization in the data center.

The Center for Internet Security, a non-profit organization that specifies best security practices for Windows and other data center software, will be floating an early version of a "hardened" set of security guidelines for VMware's ESX Server. The center calls its guides benchmarks. They are written with a focus on security performance, not speed, as with other benchmark measures.

informationweek

Full Story :
http://www.informationweek.com/news/showArticle.jhtml;jsessionid=5ZDYQL5EFESMCQSNDLRSKH0CJUNN2JVN?articleID=201804364&subSection=News

New Vulnerabilities Tested in SecureScout

❖ 16613 PHP wordwrap function, denial of service Vulnerability

The wordwrap function in PHP 4 before 4.4.8, and PHP 5 before 5.2.4, does not properly use the breakcharlen variable, which allows remote attackers to cause a denial of service (divide-by-zero error and application crash, or infinite loop) via certain arguments, as demonstrated by a 'chr(0), 0, "" argument set.

PHP versions 4.0.0 through 4.4.7 and 5.0.0 through 5.2.3 are vulnerable to the issue.

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

References:

* MISC:
http://secweb.se/en/advisories/php-wordwrap-vulnerability/
* CONFIRM:
http://www.php.net/ChangeLog-5.php#5.2.4
* CONFIRM:
http://www.php.net/releases/5_2_4.php
* SECUNIA: 26642
http://secunia.com/advisories/26642

CVE Reference: CVE-2007-3998

❖ 16612 PHP strspn and strcspn functions, information disclosure and denial of service Vulnerabilities

Multiple integer overflows in PHP 4 before 4.4.8, and PHP 5 before 5.2.4, allow remote attackers to obtain sensitive information (memory contents) or cause a denial of service (thread crash) via a large len value to the strspn or strcspn function, which triggers an out-of-bounds read.

PHP versions 4.0.0 through 4.4.7 and 5.0.0 through 5.2.3 are vulnerable to the issue.

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

References:

* MISC:
http://secweb.se/en/advisories/php-strcspn-information-leak-vulnerability/
* CONFIRM:
http://www.php.net/ChangeLog-5.php#5.2.4
* CONFIRM:
http://www.php.net/releases/5_2_4.php
* SECUNIA: 26642
http://secunia.com/advisories/26642

CVE Reference: CVE-2007-4657

❖ 16611 PHP php_openssl_make_REQ, Buffer overflow Vulnerability

Buffer overflow in the php_openssl_make_REQ function in PHP before 5.2.4 has unknown impact and attack vectors.

PHP versions 5.0.0 through 5.2.3 are vulnerable to the issue.

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

References:

* CONFIRM:
http://www.php.net/ChangeLog-5.php#5.2.4
* CONFIRM:
http://www.php.net/releases/5_2_4.php
* SECUNIA: 26642
http://secunia.com/advisories/26642

CVE Reference: CVE-2007-4662

❖ 16610 PHP "Improved fix for MOPB-03-2007" Vulnerability

Unspecified vulnerability in PHP before 5.2.4 has unknown impact and attack vectors, related to an "Improved fix for MOPB-03-2007,".

PHP versions 5.0.0 through 5.2.3 are vulnerable to the issue.

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

References:

* CONFIRM:
http://www.php.net/ChangeLog-5.php#5.2.4
* CONFIRM:
http://www.php.net/releases/5_2_4.php

CVE Reference: CVE-2007-4670

❖ 16609 PHP symlink, bypass safe_mode and open_basedir restrictions Vulnerability

PHP before 5.2.4 might allow local users to bypass open_basedir restrictions via a session file that is a symlink.

PHP versions 5.0.0 through 5.2.3 are vulnerable to the issue.

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

References:

* CONFIRM:
http://www.php.net/ChangeLog-5.php#5.2.4
* CONFIRM:
http://www.php.net/releases/5_2_4.php
* SECUNIA: 26642
http://secunia.com/advisories/26642

CVE Reference: CVE-2007-4652

❖ 16608 PHP MySQL LOCAL INFILE operations, bypass safe_mode and open_basedir restrictions Vulnerability

The MySQL and MySQLi extensions in PHP 4 before 4.4.8, and PHP 5 before 5.2.4, allow remote attackers to bypass safe_mode and open_basedir restrictions via MySQL LOCAL INFILE operations, as demonstrated by a query with LOAD DATA LOCAL INFILE.

PHP versions 4.0.0 to 4.4.7 and 5.0.0 through 5.2.3 are vulnerable to the issue.

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

References:

* MISC:
http://secweb.se/en/advisories/php-mysql-safe-mode-bypass-vulnerability/
* CONFIRM:
http://www.php.net/ChangeLog-5.php#5.2.4
* CONFIRM:
http://www.php.net/releases/5_2_4.php
* SECUNIA: 26642
http://secunia.com/advisories/26642

CVE Reference: CVE-2007-3997

❖ 16607 PHP php_value directives in .htaccess, bypass safe_mode and open_basedir restrictions Vulnerability

The session_save_path, ini_set, and error_log functions in PHP 4.4.7 and earlier, and PHP 5 5.2.3 and earlier, when invoked from a .htaccess file, allow remote attackers to bypass safe_mode and open_basedir restrictions and possibly execute arbitrary commands via php_value directives in .htaccess.

PHP versions 4.0.0 to 4.4.7 and 5.0.0 through 5.2.3 are vulnerable to the issue.

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

References:

* BUGTRAQ: 20070627 PHP 4/5 htaccess safemode and open_basedir Bypass
http://www.securityfocus.com/archive/1/archive/1/472343/100/0/threaded
* MISC:
http://securityreason.com/achievement_exploitalert/9
* NETVIGILANCE-UNKNOWN: 20070627 PHP 5.2.3 PHP 4.4.7, htaccess safemode and open_basedir Bypass
http://securityreason.com/achievement_securityalert/45
* CONFIRM:
http://www.php.net/ChangeLog-5.php#5.2.4
* CONFIRM:
http://www.php.net/releases/5_2_4.php
* BID: 24661
http://www.securityfocus.com/bid/24661
* SECUNIA: 26642
http://secunia.com/advisories/26642
* NETVIGILANCE-UNKNOWN: 2831
http://securityreason.com/securityalert/2831
* XF: php-htaccess-security-bypass(35102)
http://xforce.iss.net/xforce/xfdb/35102

CVE Reference: CVE-2007-3378

❖ 16606 PHP libgd multiple integer overflows Vulnerability

Multiple integer overflows in libgd in PHP before 5.2.4 allow remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a large srcW or srcH value to the gdImageCopyResized function, or a large sy (height) or sx (width) value to the gdImageCreate or the gdImageCreateTrueColor function.

PHP versions 5.0.0 through 5.2.3 are vulnerable to the issue.

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

References:

* MISC:
http://secweb.se/en/advisories/php-imagecopyresized-integer-overflow/
* MISC:
http://secweb.se/en/advisories/php-imagecreatetruecolor-integer-overflow/
* CONFIRM:
http://www.php.net/ChangeLog-5.php#5.2.4
* CONFIRM:
http://www.php.net/releases/5_2_4.php
* SECUNIA: 26642
http://secunia.com/advisories/26642

CVE Reference: CVE-2007-3996

❖ 16605 PHP "zend_alter_ini_entry" memory_limit interruption Vulnerability

The zend_alter_ini_entry function in PHP before 5.2.4 does not properly handle an interruption to the flow of execution triggered by a memory_limit violation, which has unknown impact and attack vectors.

PHP versions 5.0.0 through 5.2.3 are vulnerable to the issue.

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

References:

* CONFIRM:
http://www.php.net/ChangeLog-5.php#5.2.4
* CONFIRM:
http://www.php.net/releases/5_2_4.php
* SECUNIA: 26642
http://secunia.com/advisories/26642

CVE Reference: CVE-2007-4659

❖ 16604 PHP "money_format" format string Vulnerability

The money_format function in PHP before 5.2.4 permits multiple %i and %n tokens, which has unknown impact and attack vectors, possibly related to a format string vulnerability.

PHP versions 5.0.0 through 5.2.3 are vulnerable to the issue.

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

References:

* CONFIRM:
http://www.php.net/ChangeLog-5.php#5.2.4
* CONFIRM:
http://www.php.net/releases/5_2_4.php
* SECUNIA: 26642
http://secunia.com/advisories/26642

CVE Reference: CVE-2007-4658

New Vulnerabilities found this Week

Apple iTunes Music File Buffer Overflow Vulnerability

"Execution of arbitrary code"

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

The vulnerability is caused due to an unspecified boundary error when processing album cover art. This can be exploited to cause a buffer overflow via a specially crafted music file.

Successful exploitation may allow execution of arbitrary code.

The vulnerability is reported in versions prior to 7.4.

References:
http://docs.info.apple.com/article.html?artnum=306404

Cisco Catalyst Content Switching Modules Denial of Service Vulnerabilities

"Denial of Service"

Two vulnerabilities have been reported in the Cisco Catalyst Content Switching Modules (CSM) and Cisco Catalyst Content Switching Module with SSL (CSM-S), which can be exploited by malicious people to cause a DoS (Denial of Service).

1) An unspecified error exists when processing certain TCP packets that were received out of order. This can be exploited to cause a high CPU load or a device reload due to a FPGA4 exception with icp.fatPath length error by sending specially crafted TCP packets to a vulnerable system.

2) An unspecified error exists within the "service termination" option, which can be exploited to cause a PGA4 exception 1 IDLE error under a high network load by sending specially crafted TCP packets to a vulnerable system.

Vulnerability #1 is reported in CSM 4.2 prior to 4.2.3a and CMS-S 2.1prior to 2.1.2a.

Vulnerability #2 is reported in CSM 4.2 prior to 4.2.7 and CMS-S 2.1 prior to 2.1.6.

References:
http://www.cisco.com/en/US/products/products_security_advisory09186a00808b4d3b.shtml

Cisco Video Surveillance IP Gateway and Services Platform Authentication Bypass

"Gain administrative shell access"

Some vulnerabilities have been reported in Cisco Video IP Gateway and Services Platform, which can be exploited by malicious people to bypass certain security restrictions and compromise a vulnerable system.

1) The telnet service of the Cisco Video Surveillance IP Gateway video encoders and decoders does not authenticate connecting users. This can be exploited to gain administrative shell access by connecting to the vulnerable service.

2) The Cisco Video Surveillance Services Platform and Integrated Services Platform devices contain a default password for the "sypixx" and "root" accounts. This can be exploited to gain administrative shell access by connecting to the vulnerable service, but requires knowledge of the default password.

The vulnerabilities are reported in:
* Cisco Video Surveillance IP Gateway Encoder/Decoder (Standalone and Module) firmware version 1.8.1 and earlier
* Cisco Video Surveillance SP/ISP Decoder Software firmware version 1.11.0 and earlier
* Cisco Video Surveillance SP/ISP firmware version 1.23.7 and earlier

References:
http://www.cisco.com/en/US/products/products_security_advisory09186a00808b4d38.shtml

Apple AirPort Extreme Base Station IPv6 Type 0 Route Headers Denial of Service

"Denial of Service"

A security issue has been reported in Apple AirPort Extreme Base Station, which can be exploited by malicious people to cause a DoS (Denial of Service).

The security issue is caused due to an error within the processing of packets with IPv6 type 0 route headers. This can be exploited to cause a DoS due to high network traffic by sending specially crafted IPv6 packets to vulnerable systems.

The security issue is reported in firmware versions prior to 7.2.1.

NOTE: This security issue does reportedly not affect the Gigabit Ethernet version of AirPort Extreme Base Station with 802.11n*.

References:
http://docs.info.apple.com/article.html?artnum=306375

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