

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

TJX and what really happened. Third party and risks. Biometrics on the way. Look out for IE 7 beta.

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

❖ Why Encryption Didn't Save TJX

TJX: It's the target of the largest known customer record theft of all time, and it's a case in point that encryption is not a silver bullet.

This is the heart of the encryption problem, quoted from the 10-K filing The TJX Companies made to the Securities and Exchange Commission:

"Despite our masking and encryption practices on our Framingham system in 2006,

the technology utilized in the Computer Intrusion during 2006 could have enabled the Intruder to steal payment card data from our Framingham system during the payment card issuer's approval process, in which data (including the track 2 data) is transmitted to payment card issuer's without encryption. Further, we believe that the Intruder had access to the decryption tool for the encryption software utilized by TJX."

Encryption has no value when data isn't encrypted, obviously, but credit cards can't be processed when their numbers are encrypted. Hence, a smart crook will seek a way to get the data during that window of time when it's in that state of being "in the clear"—that is, unencrypted.

TJX's intruder also had a backup plan if data in the clear wasn't attainable: namely, the decryption key.

Eweek.com

Full Story :

<http://www.eweek.com/article2/0,1895,2109742,00.asp>

❖ **How SOA increases your security risk**

Service-oriented architecture changes the security equation by introducing a greater reliance on third parties for application development and operation. But according to Ray Wagner, managing vice president of information security and privacy at Gartner Inc., this is a matter of degree rather than an introduction of a totally new security exposure.

For instance, an SOA application may depend on a Web-based third-party service to provide vital functionality, with obvious security implications. But thousands of users already do this when they activate Microsoft's automatic updates.

"Ultimately, it's a matter of trust," he says. "You decide whether you trust Microsoft to send you good code. Then the computer checks that it has received what Microsoft sent, using cryptographic operations like hashes and digital signatures."

SOA may increase the number of these exchanges hugely. "Doing this hundreds of times an hour may have implications for computing loads, but it really is just a change of degree," not a qualitative change, Wagner says.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=networking_and_internet&articleId=9015145&taxonomyId=16

❖ **Biometrics leaders celebrate the formation of the United Kingdom Biometrics Institute UKBI**

There are increasing opportunities for successfully deploying biometrics technologies, not just in current high profile applications such as the National ID Card Programme, but in the financial sector, in healthcare, in securing documents and, indeed, in any situation

where a high degree of confidence in individual identity is important.

Prominent figures from the biometrics research and technologies sectors will meet at the University of Kent's Canterbury campus on Monday 2 April to celebrate the formation of the United Kingdom Biometrics Institute (UKBI).

Initiated by the University's Department of Electronics, and supported by Kent Enterprise, UKBI will aim to enhance the productive exchange of knowledge and expertise in the UK across all stakeholders, including the University's researchers, the biometrics industrial sector and potential end-users; and to provide leading-edge solutions to emerging and future market needs.

Securitypark.net

Full Story :

<http://www.securitypark.co.uk/article.asp?articleid=26612&CategoryID=1>

❖ **Malware disguising itself as IE 7 beta download**

If you receive an e-mail offering a download of Internet Explorer 7 Beta 2, delete it. A new virus is making the rounds that comes disguised as a test version of Microsoft Corp.'s current Web browser.

Security experts reported no widespread damage Friday morning, but they said the virus is notable for a couple of reasons. The e-mail includes a convincing graphic that looks like it could really be from Microsoft, and the virus is delivered when recipients click on a link rather than in an attachment, which makes it harder to stop it from reaching in-boxes.

"The idea of sending a link seems to be a trend among attackers; it's still fairly new and it works much better than sending a file," said Mikko Hypponen, chief research officer at F-Secure Corp.

The e-mails carry the subject line "Internet Explorer 7 Downloads" and appear to come from admin@microsoft.com. They include a blue, Microsoft-style graphic offering a download of IE 7 beta 2. Clicking the graphic will download an executable file called IE 7.exe.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9015142&taxonomyId=17&intsrc=kc_top

New Vulnerabilities Tested in SecureScout

❖ **17738 PHP "mail()", "ibase*" functions, buffer overflow Vulnerabilities**

A vulnerability has been reported in PHP, which can be exploited by malicious people to execute arbitrary code.

Boundary errors exist within the "mail()" and the "ibase_add_user()",

"ibase_delete_user()", and "ibase_modify_user()" functions and can be exploited to cause buffer overflows.

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:

Original advisory:

<http://www.php.net/ChangeLog-5.php#5.2.1>

http://www.php.net/releases/5_2_1.php

CVE Reference: [CVE-2007-0906](#)

❖ 17739 PHP "odbc_result_all()" function, format string Vulnerability

A vulnerability has been reported in PHP, which can be exploited by malicious people to execute arbitrary code.

A format string error exists in the "odbc_result_all()" function. Successful exploitation may allow the execution of arbitrary code, but requires that the attacker has control over the table contents of the used database.

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:

Original advisory:

<http://www.php.net/ChangeLog-5.php#5.2.1>

http://www.php.net/releases/5_2_1.php

CVE Reference: [CVE-2007-0909](#)

❖ 17740 PHP "imap_mail_compose()" function, buffer overflow Vulnerability

A vulnerability has been reported in PHP, which can be exploited by malicious people to execute arbitrary code.

An error within the "imap_mail_compose()" function can be exploited to cause a heap based buffer overflow and may allow the execution of arbitrary code, if the function is used with untrusted input to create a new MIME message.

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:

Original advisory:

<http://www.php.net/ChangeLog-5.php#5.2.1>

http://www.php.net/releases/5_2_1.php

CVE Reference: [CVE-2007-0906](#)

❖ 17741 PHP "unserialize()" functions, code execution Vulnerability

A vulnerability has been reported in PHP, which can be exploited by malicious people to execute arbitrary code.

A vulnerability caused due to an integer overflow in the "unserialize()" function's handling of ZVAL structures can be exploited to corrupt memory and execute arbitrary code.

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: **Low**

References:

Original advisory:

<http://www.php.net/ChangeLog-5.php#5.2.1>

http://www.php.net/releases/5_2_1.php

CVE Reference: [CVE-2007-0988](#)

❖ 17742 PHP "php_binary", boundary error Vulnerability

A vulnerability has been reported in PHP, which can be exploited by malicious people to execute arbitrary code.

A boundary error in the session serialization handler "php_binary" can be exploited to expose heap memory.

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: **Low**

References:

Original advisory:

<http://www.php-security.org/MOPB/MOPB-10-2007.html>

Other references:

MILWORM:3413

[URL:http://www.milw0rm.com/exploits/3413](http://www.milw0rm.com/exploits/3413)
SUSE:SUSE-SA:2007:020
[URL:http://lists.suse.com/archive/suse-security-announce/2007-Mar/0003.html](http://lists.suse.com/archive/suse-security-announce/2007-Mar/0003.html)
BID:22805
[URL:http://www.securityfocus.com/bid/22805](http://www.securityfocus.com/bid/22805)
SECUNIA:24514
[URL:http://secunia.com/advisories/24514](http://secunia.com/advisories/24514)

CVE Reference: [CVE-2007-1380](#)

❖ **17743 PHP shared memory (shmop) functions, code execution Vulnerabilities**

A vulnerability has been reported in PHP, which can be exploited by malicious people to execute arbitrary code.

Errors in the verification of resource types within the shared memory (shmop) functions can be exploited to read or write to arbitrary memory addresses.

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:

Original advisory:
<http://www.php-security.org/MOPB/MOPB-15-2007.html>

Other references:
MILWORM:3426
[URL:http://www.milw0rm.com/exploits/3426](http://www.milw0rm.com/exploits/3426)
MILWORM:3427
[URL:http://www.milw0rm.com/exploits/3427](http://www.milw0rm.com/exploits/3427)
BID:22862
[URL:http://www.securityfocus.com/bid/22862](http://www.securityfocus.com/bid/22862)
OSVDB:32781
[URL:http://www.osvdb.org/32781](http://www.osvdb.org/32781)

CVE Reference: [CVE-2007-1376](#)

❖ **17744 PHP "zip" extension, boundary error Vulnerability**

A vulnerability has been reported in PHP, which can be exploited by malicious people to execute arbitrary code.

A boundary error within the PHP 5 "zip" extension can be exploited to cause a stack-based overflow by passing an overly long string to the "zip:" URL wrapper.

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:

Original advisory:

<http://www.php-security.org/MOPB/MOPB-16-2007.html>

CVE Reference:

❖ **17745 PHP filtering mechanism can be bypassed, possible XSS Vulnerability**

A vulnerability has been reported in PHP, which can be exploited by malicious people to launch cross site scripting attacks.

If the "FILTER_SANITIZE_STRING" filter of ext/filter is used in combination with the "FILTER_FLAG_STRIP_LOW " flag, the filtering mechanism can be bypassed via certain low ASCII characters after opening brackets to e.g. conduct cross-site scripting attacks.

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: **Low**

References:

Original advisory:

<http://www.php-security.org/MOPB/MOPB-18-2007.html>

CVE Reference: [CVE-2007-1454](#)

❖ **17746 PHP "FILTER_VALIDATE_INT" filter, buffer underflow Vulnerability**

A vulnerability has been reported in PHP, which can be exploited by malicious people to execute arbitrary code.

A buffer underflow exists within the "FILTER_VALIDATE_INT" filter of the ext/filter extension. This can be exploited to execute arbitrary code, but may require a big-endian system.

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:

Original advisory:

<http://www.php-security.org/MOPB/MOPB-19-2007.html>

Other references:

- * MISC: http://www.php.net/releases/5_2_1.php
- * BID:22922
- * URL:<http://www.securityfocus.com/bid/22922>

CVE Reference: [CVE-2007-1453](#)

❖ 17937 Web Mech Designer Path Disclosure Vulnerability

REMLAB is a fully functional cross-platform web-based Battlemech designer for the tactical board game Battletech. REMLAB is built entirely on HTML, PHP, and JavaScript with AJAX functionality.

The vulnerability exists in calculate.php script which allows remote attackers to obtain sensitive information via an HTTP request to calculate.php that contains wrong value in Tonnage parameter. This causes the information to be leaked in an error message.

Test Case Impact: **Gather Info**. Vulnerability Impact: **gather info** Risk: **Low**

References:

Original Advisory:

<http://netvigilance.com/advisory0007>

Other references:

- * BUGTRAQ:20061127 REMLAB Web Mech Designer 2.0.5 Path Disclosure Vulnerability
- * URL:<http://www.securityfocus.com/archive/1/archive/1/453020/100/0/threaded>
- * FULLDISC:20061127 REMLAB Web Mech Designer 2.0.5 Path Disclosure Vulnerability
- * URL:<http://lists.grok.org.uk/pipermail/full-disclosure/2006-November/050879.html>
- * OSVDB:30264
- * URL:<http://www.osvdb.org/30264>
- * XF:remlab-calculate-path-disclosure(30538)
- * URL:<http://xforce.iss.net/xforce/xfdb/30538>

Product Home-Page:

<http://remlab.sourceforge.net/>

CVE Reference: [CVE-2006-5896](#)

New Vulnerabilities found this Week

IBM Lotus Domino Script Insertion and Buffer Overflows

“Denial of Service; Execution of arbitrary code”

Some vulnerabilities have been reported in IBM Lotus Domino and Lotus Domino Web Access, which can be exploited by malicious people to conduct script insertion attacks, cause a DoS (Denial of Service), and potentially compromise a vulnerable system.

- 1) A boundary error within the IMAP service (nimap.exe) during CRAM-MD5

authentication can be exploited to cause a buffer overflow by passing an overly long username (more than 256 bytes).

Successful exploitation crashes the service and may allow execution of arbitrary code.

2) An error in the LDAP service when handling certain requests can be exploited to cause a heap-based buffer overflow via a specially crafted request containing a string longer than 65535 bytes.

Successful exploitation crashes the service and may allow execution of arbitrary code.

3) Certain input in e-mail messages is not properly sanitized by Lotus Domino Web Access before being displayed. This can be exploited to insert arbitrary HTML and script code, which is executed in a user's browser session in context of an affected site when a malicious message is viewed.

References:

<http://www-1.ibm.com/support/docview.wss?uid=swg21257028>

<http://www-1.ibm.com/support/docview.wss?uid=swg21257248>

<http://www-1.ibm.com/support/docview.wss?uid=swg21257026>

<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=493>

<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=494>

<http://www.zerodayinitiative.com/advisories/ZDI-07-011.html>

Sun Java System Directory Server "ns-slapd" Denial of Service

"Denial of Service"

A vulnerability has been reported in Sun Java System Directory Server, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an unspecified error within the handling of certain queries, which leads to a "free()" operation being performed on uninitialised memory. This can be exploited to crash the "ns-slapd" service by sending specially crafted queries.

The vulnerability is reported in the following products for Solaris 8, 9, and 10 on Solaris SPARC and Solaris x86 Platforms, Linux, Windows, HP-UX, and AIX:

-- Native Package Versions --

* Sun ONE Directory Server 5.2

* Sun Java System Directory Server 5 2003Q4 (5.2patch1)

* Sun Java System Directory Server 5 2004Q2 (5.2patch2)

* Sun Java System Directory Server 5 2005Q1 (5.2patch3)

* Sun Java System Directory Server 5 2005Q4 (5.2patch4)

-- PatchZIP (Compressed Archive) versions --

* Sun ONE Directory Server 5.1

* Sun One Directory Server 5.2

* Sun Java System Directory Server 5.2 Patch2

* Sun Java System Directory Server 5.2 Patch3

* Sun Java System Directory Server 5.2 Patch4

References:

<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=491>
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102853-1>

PHP "unserialize()" S: Data Type Information Leak

“Disclose potentially sensitive information”

Stefan Esser has reported a vulnerability in PHP, which can be exploited by malicious people to disclose potentially sensitive information.

The vulnerability is caused due to an error within the "unserialize()" function when unserialising specially escaped S: data types. This can be exploited to e.g. disclose certain parts of the heap memory.

The vulnerability is reported in version 5.2.1.

References:

<http://www.php-security.org/MOPB/MOPB-29-2007.html>

Linux Kernel Multiple Denial of Service Vulnerabilities

“Denial of Service”

Some vulnerabilities have been reported in the Linux Kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

1) Listening IPv6 TCP sockets are incorrectly sharing the "ipv6_fl_socklist" IPv6 flowlist with child sockets. This can be exploited to e.g. cause a kernel crash by performing certain actions on IPv6 TCP sockets.

2) The "hrtimer_forward()" does not correctly check for "timer->expires" overflows on 64bit machines. This can be exploited to cause a DoS by using very large timer values.

Successful exploitation may require a 64bit machine and that high resolution timers are enabled.

3) A NULL pointer dereference within the "do_ipv6_setsockopt()" function in net/ipv6/ipv6_sockglue.c can be exploited to cause a kernel crash by calling "setsockopt()" with malicious parameters.

The vulnerabilities are reported in versions prior to 2.6.20.4.

References:

<http://marc.info/?l=linux-netdev&m=117406721731891&w=2>
<http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.20.4>
http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=233478
<http://lkml.org/lkml/2007/3/13/285>
http://bugzilla.kernel.org/show_bug.cgi?id=8155

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