netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 12

March 23, 2007

Table of Contents

Product Focus

RPC DCOM Vulnerabilities Scanner – The RPC DCOM Vulnerabilities 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 Windows RPC DCOM flaws (MS03-026 and MS03-039).

This Week in Review

Windows flaws few but severe. The ever rising security risks. New Trojan after Skype. Wi-Fi hot spots really hot.

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

- **Symantec: Windows flaws more severe**

Windows requires fewer patches and has faster patch turnaround times than some other large vendors, yet Microsoft software flaws are still more severe, according to Symantec.

In its comprehensive Internet Security Threat Report Volume XI, which covers the period from July to December 2006, Symantec said that out of 39 Microsoft vulnerabilities disclosed during this period, 12 were of high severity, 20 were of

medium severity, and seven were less severe.
By comparison, although Red Hat Linux had 208 disclosed vulnerabilities during the second half of 2006, only two were considered high severity, while 130 were medium severity and 76 low.

Apple fared better than Red Hat. Out of 43 vulnerabilities reported in Mac OS X, one was considered high severity, 31 were medium severity and 11 were low.

zdnet

Full Story :
http://news.zdnet.co.uk/security/0,1000000189,39286453,00.htm

❖ Malware danger and profitability rising

Two major new reports on computer security issues have shown a steady rise in just about every aspect of security risk, with increased danger from each vector in some way linked to financial motives.

According to Symantec's report on the threat landscape in the second half or last year, released last week, viruses, worms and trojans, exploitation of vulnerabilities, spam and phishing, spyware and data theft were all up on previous figures.

The report shows a decrease in volume of network worms, with a matching increase in the numbers of trojans seen, and also reckons that while half of the top ten malcode families are viruses and worms and half are trojans, the trojans have the edge in terms of potential to infect.

The US was again the major source of malware and spam, and although China has the lead in terms of machines infected with bots, most are controlled from the US, and the States is also home to most spam-sending bots. More detailed figures on these and many other issues can be found in the full report, which can be found here.

Virus bulletin

Full Story :
http://www.virusbtn.com/news/virus_news/2007/03_22.xml?rss

❖ Skype gets call from a Trojan

Another Trojan horse is spreading through the Internet telephone network of Skype Ltd.

The malicious code, known as both Warezov and Stration, is similar to an earlier version detected in February, but with a new URL (uniform resource locator) and a new version of the malicious code, according to an alert posted Thursday by Websense Inc.

Websense warns Skype users to watch for the message "Check up this," with a URL containing a hyperlink.

The code itself isn't self-propogating but when it runs, the URL is sent to everyone on the user's contact list.

When users click on the link, they are redirected to a site that is hosting a file named file_01.exe. Users are then prompted to run the file and if they do, several other files are downloaded and run. The downloaded files are other versions of the Waresov/Stration malicious code.

computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9014167&intsrc=news_ts_head

- **Wi-Fi worry: Laptops at risk of attack**

As communities push to turn themselves into massive wireless hot spots, unsuspecting Internet users are giving hackers nearly effortless access to their laptops and private information, authorities and high-tech security experts say.

It's a growing invasion with a twist: People who think they are signing on to the Internet through a wireless hot spot might actually be connecting to a look-alike network, created by a malicious user who can steal sensitive information, said Geoff Bickers, a special agent for the FBI's Los Angeles cyber squad.

It is not clear how many people have been victimized, and few suspects have been charged with Wi-Fi hacking. But Bickers said that over the past couple of years, these hacking techniques have become increasingly common, and they are often undetectable. The risk is especially high at cafes, hotels and airports, busy places with heavy turnover of laptop users, authorities said.

Seattle Times

Full Story :
http://seattletimes.nwsource.com/html/personaltechnology/2003631947_wifi23.html

New Vulnerabilities Tested in SecureScout

- **17349 PHP "array_user_key_compare()", Privilege escalation Vulnerability**

Stefan Esser has discovered a vulnerability in PHP, which can be exploited by malicious users to gain escalated privileges.

An error in the "array_user_key_compare()" function where key references are incorrectly destroyed can be exploited to cause memory corruption.

The vulnerability is confirmed in version 5.2.1 and also reported in version 4.4.6. 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-24-2007.html

Other references:
http://secunia.com/advisories/24542/

CVE Reference: CVE-2007-1484

❖ 17474 PHP handling of resource data, Arbitrary code execution Vulnerability

Stefan Esser has discovered a vulnerability in PHP, which can be exploited by malicious users to execute arbitrary code.

An error in the handling of resource data can be exploited to destroy and replace certain resources by interrupting the processing PHP function (e.g. functions of the GD extension). This allows read and write access to arbitrary memory addresses.

Successful exploitation of the vulnerability allows execution of arbitrary code, which can lead to security restrictions, such as the "disable_functions" directive, being bypassed.

The vulnerability is confirmed in version 5.2.1 and also reported in version 4.4.6. 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-27-2007.html
http://www.php-security.org/MOPB/MOPB-28-2007.html

Other references:
http://secunia.com/advisories/24542/

CVE Reference:

❖ 17479 PHP Interbase Extension "isc_attach_database()" Buffer Overflow Vulnerability

rgod has discovered a vulnerability in PHP's Interbase extension, which can be exploited by malicious users to gain escalated privileges.

The vulnerability is caused due to a boundary error when processing arguments passed to "isc_attach_database()" in GDS32.DLL located in the PHP directory when the Interbase extension is installed. This can be exploited to cause a stack-based buffer overflow via an overly long (greater than 260 bytes) string passed as argument to e.g. PHP's "ibase_connect()" or "ibase_pconnect()" functions and execute arbitrary code therefore bypassing security restrictions like the "disable_functions" directive.

Successful exploitation requires that the Interbase extension is installed.

The vulnerability is confirmed in version 5.2.1 and also reported in version 4.4.6. Other versions may also be affected.

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

References:

Original advisory:
http://milw0rm.com/exploits/3488

Other references:
* BUGTRAQ:20070315 PHP <= 4.4.6 ibase_connect() local buffer overflow
* URL:http://www.securityfocus.com/archive/1/archive/1/462931/100/0/threaded
* MISC: http://retrogod.altervista.org/php_446_ibase_connect_bof.html
* BID:22976
* URL:http://www.securityfocus.com/bid/22976

CVE Reference: CVE-2007-1475

❖ 17481 PHP "htmlentities()" and "htmlspecialchars()" Buffer Overflows Vulnerabilities

Some vulnerabilities have been reported in PHP, which can be exploited by malicious people to cause a DoS (Denial of Service) or potentially compromise a vulnerable system.

The vulnerabilities are caused due to boundary errors within the "htmlentities()" and "htmlspecialchars()" functions. If a PHP application uses these functions to process user-supplied input, this can be exploited to cause a heap-based buffer overflow by passing specially crafted data to the affected application.

Successful exploitation may allow execution of arbitrary code, but requires that the UTF-8 character set is selected.

The vulnerability is confirmed in version 5.x < 5.2.0 and also reported in version 4.4.6. Other versions may also be affected.

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

References:

Original advisory:
http://www.ubuntu.com/usn/usn-375-1
http://www.hardened-php.net/advisory_132006.138.html

CVE Reference: CVE-2006-5465

❖ 17529 PHP session extension, bypass "safe_mode" and "open_basedir" protection Vulnerability

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

The "safe_mode" and "open_basedir" protection mechanisms can be bypassed via the session extension.

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

Other references:
OPENPKG:OpenPKG-SA-2007.010
URL:http://www.openpkg.com/security/advisories/OpenPKG-SA-2007.010.html
BID:22496
URL:http://www.securityfocus.com/bid/22496
FRSIRT:ADV-2007-0546
URL:http://www.frsirt.com/english/advisories/2007/0546
SECUNIA:24089
URL:http://secunia.com/advisories/24089

CVE Reference: CVE-2007-0905

❖ 17555 PHP extensions, buffer overflows Vulnerability

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

Unspecified overflows can be exploited to cause a stack corruption in the "session", "zip", "imap", and "sqlite" extensions.

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

❖ 17556 PHP stream filters, boundary error Vulnerability

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

A boundary error within the stream filters can be exploited to cause a buffer overflow.

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

❖ 17557 PHP "str_replace()" function, integer overflow Vulnerability

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

An integer overflow exists in the "str_replace()" function. This can be exploited to trigger an error when allocating memory and potentially allows the execution of arbitrary code, if the function is used on long, untrusted strings.

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

❖ **17736 PHP "php_set_session_var()" function, memory disclosure Vulnerability**

A vulnerability has been reported in PHP, which can be exploited by malicious people to disclose sensitive information.

A boundary error in a call to "php_set_session_var()" when importing malicious WDDX data containing a numerical key can be exploited to disclose random 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.net/ChangeLog-5.php#5.2.1
http://www.php.net/releases/5_2_1.php

CVE Reference: CVE-2007-0908

❖ **17737 PHP *print() function, format string error 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 *print() functions on 64-bit systems.

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

New Vulnerabilities found this Week

Asterisk SIP Response Code Denial of Service
"Denial of Service"

qwerty1979 has reported a vulnerability in Asterisk, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the processing of SIP replies from a remote system and can be exploited to crash the service via the remote system sending a SIP reply containing SIP Response code 0.

The vulnerability is reported to affect only the 1.4.x branch.

References:
http://www.sineapps.com/news.php?rssid=1707
http://bugs.digium.com/view.php?id=9313

Squid TRACE Request Denial of Service Vulnerability
"Denial of Service"

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

The vulnerability is caused due to an error within the processing of TRACE requests in squid/src/client_side.c. This can be exploited to crash the service via a specially crafted TRACE request.

The vulnerability is reported in all Squid 2.6 versions up to 2.6.STABLE11.

References:
http://www.squid-cache.org/Advisories/SQUID-2007_1.txt

OpenOffice.org Multiple Vulnerabilities
"Execution of arbitrary code"

Some vulnerabilities have been reported in OpenOffice.org, which potentially can be exploited by malicious people to compromise a user's system.

1) Several vulnerabilities within the libwpd library used by OpenOffice.org can be exploited to cause heap-based buffer overflows and may allow the execution of arbitrary code by e.g. tricking a user into opening a specially crafted WordPerfect document.

2) A boundary error within the StarCalc parser can be exploited to cause a stack-based buffer overflow and may allow execution of arbitrary code by e.g. tricking a user into opening a specially crafted document.

3) Shell meta characters are not correctly escaped, which can be exploited to inject and execute arbitrary shell commands by e.g. tricking a user into opening a specially crafted document and clicking a malicious link.

References:
http://www.debian.org/security/2007/dsa-1270
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=490

Asterisk SIP INVITE Denial of Service Vulnerability
"Denial of Service"

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

The vulnerability is caused due to an error within the handling of certain SIP INVITE messages. This can be exploited to crash the server by sending a SIP INVITE message with 2 SDP headers, where the second header contains an invalid IP address.

Successful exploitation requires that the callee is an invalid dailplan or user.

The vulnerability is reported in versions 1.2.14, 1.2.15, 1.2.16, and 1.4.1. Prior versions may also be affected.

References:
http://www.sineapps.com/news.php?rssid=1707
http://lists.grok.org.uk/pipermail/full-disclosure/2007-March/053052.html

Cisco IP Phone 7940/7960 SIP INVITE Denial of Service Vulnerability
"Denial of Service"

A vulnerability has been reported in Cisco IP Phone 7940 and 7960, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error within the handling of certain SIP INVITE messages. This can be exploited to reboot the device by sending a specially crafted INVITE message with a malformed "sipURI" field of the Remote-Party-ID.

The vulnerability is reported in devices running firmware POS3-07-4-00.

References:
http://www.cisco.com/en/US/products/products_security_response09186a00808075ad.html

Microsoft Windows NDISTAPI.SYS Denial of Service
"Denial of Service"

Rubén Santamarta has reported a vulnerability in Microsoft Windows, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the handling of data sent to the "\Device\NdisTapi" device. This can be exploited to crash a vulnerable system by sending arbitrary data to the said device.

The vulnerability is reported in Microsoft Windows XP SP2 and Microsoft Windows 2003 Server SP1. Other versions may also be affected.

References:
http://www.reversemode.com/index.php?option=com_remository&Itemid=2&func=fileinfo&id=47

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