netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 46

November 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

Time to look at DNS traffic. China to take big leap in security spendings. So easy is it. Be aware of security problems with security software.

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

- **Defense-in-depth starts with DNS**

How do you stop computers on your network from becoming a part of massive botnets? Maybe you just trust that your desktop anti-virus definitions are up-to-date. When was the last time you looked at the DNS traffic patterns on your network? Perhaps you just break out WireShark from time to time to debug problems. Do you block outbound requests to external DNS servers on your firewall? If you're anything like the IT folks I talk to, you don't block DNS, nor do you pay any special attention to it. The general sentiment from the people I talk with is that "as long as my DNS works,

it's fine."

That needs to change. DNS needs to be considered a critical layer in practicing defense-in-depth security.

ZDnet

Full Story :
http://blogs.zdnet.com/security/?p=679

❖ China's network security market heating up

China's network security market chalked up sales of ¥1.782bn (£116m) in the most recent quarter, up 24.3 per cent year on year, according to new research.
CCID Consulting said that security consulting, security management monitoring and grade evaluation have become the important driving forces in the market.
The report added that "frequent accidents" have compelled small and medium sized firms to devote more funds to network security.
Firewalls remain the dominant technology products, but unified threat management, content security management and Secure Sockets Layer virtual private networks are also significant.

vnunet

Full Story :
http://www.vnunet.com/vnunet/news/2204094/china-network-security-market

❖ Expert scares world with VoIP hacking proof

An expert has released a proof-of-concept program to show how easy it would be for criminals to eavesdrop on the VoIP-based phone calls of any company using the technology.
Called SIPtap, the software is able to monitor multiple Voice-over-IP (VoIP) call streams, listening in and recording them for remote inspection as .wav files. All that the criminal would need would be to infect a single PC inside the network with a Trojan incorporating these functions, although the hack would work at ISP level as well.

techworld

Full Story :
http://www.techworld.com/security/news/index.cfm?newsID=10736&pagtype=all

❖ Is security software becoming a security risk?

Is the software we're using to protect ourselves from online attacks becoming a liability?

That's what Thierry Zoller believes. For the past two years, the security engineer for n.runs has taken a close look at the way antivirus software inspects email traffic, and he thinks companies that try to improve security by checking data with more than one antivirus engine may actually be making things worse. Why? Because bugs in the "parser"

software used to examine different file formats can easily be exploited by attackers, so increasing your use of antivirus software increases the chances that you could be successfully attacked.

Computerworld

Full Story :
http://computerworld.co.nz/news.nsf/scrt/4EBFA4846D9A809ACC25739B000F4241

New Vulnerabilities Tested in SecureScout

- **17763 PHP substr_compare function, interger overflow Vulnerability**

Integer overflow in the substr_compare function in PHP allows context-dependent attackers to read sensitive memory via a large value in the length 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**

References:

* MILW0RM: 3424
http://www.milw0rm.com/exploits/3424
* MISC:
http://www.php-security.org/MOPB/MOPB-14-2007.html
* CONFIRM:
http://us2.php.net/releases/5_2_2.php
* DEBIAN: DSA-1283
http://www.debian.org/security/2007/dsa-1283
* GENTOO: GLSA-200703-21
http://security.gentoo.org/glsa/glsa-200703-21.xml
* MANDRIVA: MDKSA-2007:187
http://www.mandriva.com/security/advisories?name=MDKSA-2007:187
* 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: 22851
http://www.securityfocus.com/bid/22851
* OSVDB: 32780
http://www.osvdb.org/32780
* SECUNIA: 24606
http://secunia.com/advisories/24606
* SECUNIA: 25062
http://secunia.com/advisories/25062
* SECUNIA: 25057
http://secunia.com/advisories/25057
* SECUNIA: 25056
http://secunia.com/advisories/25056
* SECUNIA: 26895
http://secunia.com/advisories/26895

CVE Reference: CVE-2007-1375

❖ 16780 PHP iconv_* functions, multiple denial of service Vulnerabilities

PHP allows context-dependent attackers to cause a denial of service (application crash) via a long string in the out_charset parameter to the iconv function; or a long string in the charset parameter to the iconv_mime_decode_headers, iconv_mime_decode, or iconv_strlen function. NOTE: this might not be a vulnerability in most web server environments that support multiple threads, unless these issues can be demonstrated for code execution.

PHP versions 5.x through 5.2.4 are vulnerable to the issue.

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

References:

* BUGTRAQ: 20070906 PHP <= 5.2.4 multiple Iconv functions denial of service
http://www.securityfocus.com/archive/1/archive/1/478730/100/0/threaded
* GENTOO: GLSA-200710-02
http://www.gentoo.org/security/en/glsa/glsa-200710-02.xml
* SECUNIA: 27102
http://secunia.com/advisories/27102
* SREASON: 3122
http://securityreason.com/securityalert/3122

CVE Reference: CVE-2007-4840

❖ 16779 PHP iconv_substr function, denial of service Vulnerability

The iconv_substr function in PHP allows context-dependent attackers to cause a denial of service (application crash) via a long string in the charset parameter, probably also requiring a long string in the str parameter; or a denial of service (temporary application hang) via a long string in the str parameter. NOTE: this might not be a vulnerability in most web server environments that support multiple threads, unless these issues can be demonstrated for code execution.

PHP versions 5.x through 5.2.4 are vulnerable to the issue.

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

References:

* BUGTRAQ: 20070905 PHP <=5.2.4 iconv_substr() denial of service
http://www.securityfocus.com/archive/1/archive/1/478637/100/0/threaded
* GENTOO: GLSA-200710-02

http://www.gentoo.org/security/en/glsa/glsa-200710-02.xml
* SECUNIA: 27102
http://secunia.com/advisories/27102
* SREASON: 3115
http://securityreason.com/securityalert/3115

CVE Reference: CVE-2007-4783

❖ 16778 PHP dl function, denial of service Vulnerability

The dl function in PHP allows context-dependent attackers to cause a denial of service (application crash) via a long string in the library parameter. NOTE: there are limited usage scenarios under which this would be a vulnerability.

PHP versions 5.x through 5.2.4 are vulnerable to the issue.

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

References:

* BUGTRAQ: 20070910 /* PHP <=5.2.4 open_basedir bypass & code exec & denial of service errata ... working on windows too .. */
http://www.securityfocus.com/archive/1/archive/1/478988/100/0/threaded
* BUGTRAQ: 20070910 PHP <=5.2.4 open_basedir bypass & code exec & denial of service
http://www.securityfocus.com/archive/1/archive/1/478985/100/0/threaded
* GENTOO: GLSA-200710-02
http://www.gentoo.org/security/en/glsa/glsa-200710-02.xml
* BID: 26403
http://www.securityfocus.com/bid/26403
* FRSIRT: ADV-2007-3825
http://www.frsirt.com/english/advisories/2007/3825
* SECUNIA: 27102
http://secunia.com/advisories/27102
* SREASON: 3133
http://securityreason.com/securityalert/3133

CVE Reference: CVE-2007-4887

❖ 16777 Vulnerability in DNS Could Allow Spoofing (MS07-062/941672) (Remote File Checking)

A spoofing vulnerability exists in Windows DNS Servers. The vulnerability could allow non-privileged users to send malicious responses to DNS requests, thereby spoofing or redirecting Internet traffic from legitimate locations.

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

References:

* BUGTRAQ: 20071113 After 6 months - fix available for Microsoft DNS cache poisoning attack
http://www.securityfocus.com/archive/1/archive/1/483635/100/0/threaded
* BUGTRAQ: 20071114 Predictable DNS transaction IDs in Microsoft DNS Server
http://www.securityfocus.com/archive/1/archive/1/483698/100/0/threaded
* MISC:
http://www.trusteer.com/docs/windowsdns.html
* MISC:
http://www.scanit.be/advisory-2007-11-14.html
* MS: MS07-062
http://www.microsoft.com/technet/security/bulletin/ms07-062.mspx
* CERT-VN: VU#484649
http://www.kb.cert.org/vuls/id/484649
* BID: 25919
http://www.securityfocus.com/bid/25919
* FRSIRT: ADV-2007-3848
http://www.frsirt.com/english/advisories/2007/3848
* SECTRACK: 1018942
http://www.securitytracker.com/id?1018942
* SECUNIA: 27584
http://secunia.com/advisories/27584
* XF: win-dns-spoof-information-disclosure(36805)
http://xforce.iss.net/xforce/xfdb/36805

CVE Reference: CVE-2007-3898

❖ 16776 Vulnerability in Windows URI Handling Could Allow Remote Code Execution (MS07-061/943460) (Remote File Checking)

A remote code execution vulnerability exists in the way that the Windows shell handles specially crafted URIs that are passed to it. An attacker could exploit this vulnerability by including a specially crafted URI in an application or attachment, which could potentially allow remote code execution.

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

Some References:

* BUGTRAQ: 20071011 M$ will fix URI?
http://www.securityfocus.com/archive/1/archive/1/482090/100/0/threaded
* BUGTRAQ: 20071014 Third-party patch for CVE-2007-3896 (Internet Explorer 7 invalid URI handling) available
http://www.securityfocus.com/archive/1/archive/1/482292/100/0/threaded
* BUGTRAQ: 20071017 Re: Third-party patch for CVE-2007-3896, UPDATE NOW
http://www.securityfocus.com/archive/1/archive/1/482437/100/0/threaded
* BUGTRAQ: 20071004 Re: 0day: mIRC pwns Windows
http://www.securityfocus.com/archive/1/archive/1/481505/100/0/threaded
* BUGTRAQ: 20071004 Re[2]: 0day: mIRC pwns Windows
http://www.securityfocus.com/archive/1/archive/1/481493/100/100/threaded
* BUGTRAQ: 20071005 RE: URI handling woes in Acrobat Reader, Netscape, Miranda, Skype
http://www.securityfocus.com/archive/1/archive/1/481624/100/0/threaded

CVE Reference: CVE-2007-3896

❖ 14058 Samba Remote Code Execution in Samba's nmbd Vulnerability

When nmbd has been configured as a WINS server, a client can send a series of name registration request followed by a specific name query request packet and execute arbitrary code.

The security issue has been fixed in version 3.0.27.

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

References:

* SECUNIA:
http://secunia.com/secunia_research/2007-90/
* MISC:
http://us1.samba.org/samba/history/security.html

CVE Reference: CVE-2007-5398

❖ 14057 Samba GETDC mailslot processing buffer overrun in nmbd Vulnerability

Processing of specially crafted GETDC mailslot requests can result in a buffer overrun in nmbd. It is not believed that that this issues can be exploited to result in remote code execution.

The security issue has been fixed in version 3.0.27.

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

References:

* SECUNIA:
http://secunia.com/secunia_research/2007-90/
* MISC:
http://us1.samba.org/samba/history/security.html

CVE Reference: CVE-2007-4572

❖ 17762 PHP ability to "clobber" certain super-global variables Vulnerability

Unspecified vulnerability in PHP allows attackers to "clobber" certain super-global variables via unspecified vectors.

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**

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
* BUGTRAQ: 20070418 rPSA-2007-0073-1 php php-mysql php-pgsql
http://www.securityfocus.com/archive/1/archive/1/466166/100/0/threaded
* CONFIRM:
http://www.php.net/ChangeLog-5.php#5.2.1
* CONFIRM:
http://www.php.net/releases/5_2_1.php
* 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
* CONFIRM:
https://issues.rpath.com/browse/RPL-1268

CVE Reference: CVE-2007-0910

❖ 17761 PHP sapi_header_op function, buffer underflow Vulnerability

Buffer underflow in PHP allows attackers to cause a denial of service via unspecified vectors involving the sapi_header_op function.

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:

* BUGTRAQ: 20070227 rPSA-2007-0043-1 php php-mysql php-pgsql
http://www.securityfocus.com/archive/1/archive/1/461462/100/0/threaded
* CONFIRM:
http://www.php.net/ChangeLog-5.php#5.2.1
* CONFIRM:
http://www.php.net/releases/5_2_1.php
* 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

CVE Reference: CVE-2007-0907

New Vulnerabilities found this Week

BitDefender Online Scanner ActiveX Control Buffer Overflow

"heap-based buffer overflow; execution of arbitrary code"

Greg Linares has reported a vulnerability in BitDefender Online Scanner, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an input validation error within the OScan8.ocx / OScan81.ocx ActiveX control when handling arguments passed to the "InitX()" method. This can be exploited to cause a heap-based buffer overflow by prepending two "%" characters to the argument of the affected method.

Successful exploitation allows execution of arbitrary code.

The vulnerability is reported in version 8.0. Other versions may also be affected.

References:
http://research.eeye.com/html/advisories/published/AD20071120.html

Linksys WAG54GS Cross-Site Scripting and Cross-Site Request Forgery Vulnerabilities

"Cross-site scripting; Cross-site request forgery"

Adrian Pastor has reported some vulnerabilities in Linksys WAG54GS, which can be exploited by malicious people to conduct cross-site scripting and cross-site request forgery attacks.

1) Input passed to the "devname", "snmp_getcomm", "snmp_setcomm", and "c4_trap_ip_" parameters in setup.cgi 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.

2) The application allows users to perform certain actions via HTTP requests without performing any validity checks to verify the request. This can be exploited to e.g. perform certain administrative actions by enticing a logged-in administrator to visit a malicious site.

The vulnerabilities are reported in firmware version 1.00.06. Other versions may also be affected.

References:
http://www.gnucitizen.org/blog/persistent-xss-and-csrf-on-wireless-g-adsl-gateway-with-speedbooster-wag54gs

phpMyAdmin "convcharset" Cross-Site Scripting

"Cross-site scripting attacks"

Tim Brown has discovered a vulnerability in phpMyAdmin, which can be exploited by malicious people to conduct cross-site scripting attacks.

Input passed to the "convcharset" parameter in index.php (when "auth_type" in the configuration is set to "cookie") 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 vulnerability is confirmed in version 2.11.2.1. Prior versions may also be affected.

References:
http://www.phpmyadmin.net/home_page/security.php?issue=PMASA-2007-8

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 and by malicious people to cause a DoS (Denial of Service).

1) An error within the "wait_task_stopped()" function can be exploited to cause a DoS by manipulating the state of a child process while the parent is waiting for the state to change (e.g. the parent is inside "wait()" or "waitpid()").

2) An NULL-pointer dereference error exists within the "tcp_sacktag_write_queue()" function when processing ACK packets. This can be exploited to crash an affected system via specially crafted ACK packets.

The vulnerabilities are reported in versions prior to 2.6.23.8.

References:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.23.8

MySQL InnoDB Denial of Service Vulnerability
"Denial of Service"

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

The vulnerability is caused due to an assertion error within the InnoDB engine and can be exploited to crash the database server via certain "CONTAINS" statements.

Successful exploitation requires "ALTER" privileges.

The vulnerability is reported in version 5.1.17, 5.0.44, and 4.1.20. Other versions may also be affected.

References:
http://bugs.mysql.com/bug.php?id=32125

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