netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 15

April 13, 2007

Table of Contents

Product Focus

Spida Digispid Worm Scanner – The Spida Digispid Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are prone any of the Microsoft Java Virtual Machine Vulnerabilities (MS02-069).

This Week in Review

How to handle the Windows DNS bug. Unify IT and building security management. Rootkits becoming more virulent. Education helps against malware.

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

- **FAQ: Here's the deal on the Windows DNS bug**

If this is how every month in 2007 is going to go, anyone using Windows might want to set up a cot next to the computer right now: you may be working overtime, all the time, patching zero-day vulnerabilities.

Last month it was the animated cursor bug in Windows; this month it's a hole in Microsoft's server software line. What do they have in common? Both are critical

flaws, both were being exploited by attackers before the bug was acknowledged by Microsoft -- and attacks amped up within days -- and both deserve Computerworld's FAQ treatment.

This FAQ spells out the at-risk population, details the bug and ticks off the stop-gap measures that are -- until Microsoft actually fixes the flaw -- the only defense.

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9016987&taxonomyId=17&intsrc=kc_top

- **Experts urge firms to take a unified approach to IT and building security management**

Converging IT and building security will result in cost savings and efficiency gains, according to experts at a Forrester forum in Amsterdam
The barriers between IT and physical security are beginning to dissolve, bringing potential business benefits to organisations, according to experts at the Forrester security forum EMEA in Amsterdam.

Claudia Natanson, chief information security officer for drinks giant Diageo, argued that companies would be able to roll out technologies like identity management systems more cheaply and efficiently if IT and building security were put under a single management structure.

“Physical security is going – there’s no such thing anymore,” she argued. “When we are looking at the CCTV cameras in our massive warehouses, we need to be efficient, so it’s our duty to look at the things that can help the organisation achieve this...[like] security convergence.”

itweek

Full Story :
http://www.itweek.co.uk/itweek/news/2188036/physical-security-convergence

- **Uber-rootkits challenge security community**

Rootkits are rapidly becoming more prolific and more virulent, IT security experts warned today.

McAfee reported that rootkits, including malware such as Trojans, worms and viruses that actively conceal their existence at a low level within operating systems, are becoming more prevalent and more sophisticated.

The security firm warned that rootkit techniques will continue to challenge the security community as hackers create more potent and more virulent strains.

"The number of rootkits submitted to McAfee Avert Labs in the first quarter of 2007, compared to the first quarter of 2006, has decreased by 15 per cent demonstrating that

we are getting better at capturing existing families and existing techniques," said Jeff Green, senior vice president at McAfee Avert Labs.

Vnunet.com

Full Story :
http://www.vnunet.com/vnunet/news/2188053/uber-rootkits-challenge

- **Preventing malware with tools and security education**

Because of the incredible variety and complexity of a malware infection, prevention is the most effective way to battle malware. In previous chapters of this Windows Security Threats All-in-One Guide, we discussed the different types of malware and the different methods to remove them. Since removal can be a tedious -- and potentially impossible -- endeavour, taking any and all steps necessary to prevent infection can save both security administrators and users a lot of time and trouble.

Unlike malware removal, which often requires specific understanding of how a malware infection can impact a given system, various security prevention techniques will effectively block malware regardless of its particular characteristics. Of course, some types of malware can sneak past any defenses, so it is best to apply as many prevention techniques as possible.

Computerweekly.com

Full Story :
http://www.computerweekly.com/Articles/2007/04/17/223174/preventing-malware-with-tools-and-security-education.htm

New Vulnerabilities Tested in SecureScout

- **16477 Vulnerability in Universal Plug and Play Could Allow Remote Code Execution (MS07-019/931261) (Remote File Checking)**

A remote code execution vulnerability exists in the Universal Plug and Play service in the way that it handles specially crafted HTTP requests. An attacker who has successfully exploited this vulnerability could run arbitrary code in the context of local service.

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

References:

Original advisory:
MS07-019
http://www.microsoft.com/technet/security/bulletin/ms07-019.mspx

CVE Reference: CVE-2007-1204

- **16478 Vulnerability in Microsoft Agent Could Allow Remote Code**

Execution (MS07-020/932168) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Agent in the way that it handles certain specially crafted URLs.

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

References:

Original advisory:
MS07-020
http://www.microsoft.com/technet/security/bulletin/ms07-020.mspx

Other references:
* MISC: http://secunia.com/secunia_research/2006-74/advisory/

CVE Reference: CVE-2007-1205

❖ 16479 MsgBox (CSRSS) Remote Code Execution Vulnerability (MS07-021/930178) (Remote File Checking)

A remote code execution vulnerability exists in the Windows Client/Server Run-time Subsystem (CSRSS) process because of the way that it handles error messages. An attacker could exploit the vulnerability by constructing a specially crafted application that could potentially allow remote code execution.

Additionally, if a user viewed a specially crafted Web site, an attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

References:

Original advisory:
MS07-021
http://www.microsoft.com/technet/security/bulletin/ms07-021.mspx

Other references:
BUGTRAQ:20061221 Microsoft Windows XP/2003/Vista memory corruption 0day
#
URL:http://www.securityfocus.com/archive/1/archive/1/455061/100/0/threaded
BUGTRAQ:20061221 Re: [Full-disclosure] Microsoft Windows XP/2003/Vista memory corruption 0day
#
URL:http://www.securityfocus.com/archive/1/archive/1/455104/100/0/threaded
BUGTRAQ:20061221 Re: [Full-disclosure] Microsoft Windows XP/2003/Vista memorycorruption 0day
#
URL:http://www.securityfocus.com/archive/1/archive/1/455088/100/0/threaded
BUGTRAQ:20061222 Re: Re: [Full-disclosure] Microsoft Windows XP/2003/Vista

memory corruption 0day
#
URL:http://www.securityfocus.com/archive/1/archive/1/455158/100/0/threaded
BUGTRAQ:20061230 csrss.exe double-free vulnerability - arbitrary DWORD overwrite exploit
#
URL:http://www.securityfocus.com/archive/1/archive/1/455546/100/0/threaded
FULLDISC:20061221 Microsoft Windows XP/2003/Vista memory corruption 0day
URL:http://lists.grok.org.uk/pipermail/full-disclosure/2006-December/051394.html
MISC: http://www.determina.com/security.research/vulnerabilities/csrss-harderror.html
MISC: http://www.security.nnov.ru/Gnews944.html
MISC: http://www.security.nnov.ru/files/messagebox.c
MISC:
http://groups.google.ca/group/microsoft.public.win32.programmer.kernel/browse_thread/thread/c5946bf40f227058/7bd7b5d66a4e5aff
MISC: http://www.kuban.ru/forum_new/forum2/files/19124.html
MISC: http://isc.sans.org/diary.php?n&storyid=1965
MISC: http://research.eeye.com/html/alerts/zeroday/20061215.html
MILW0RM:2967
URL:http://milw0rm.com/exploits/2967
CONFIRM: http://blogs.technet.com/msrc/archive/2006/12/22/new-report-of-a-windows-vulnerability.aspx
BID:21688
URL http://www.securityfocus.com/bid/21688
FRSIRT:ADV-2006-5120
URL:http://www.frsirt.com/english/advisories/2006/5120
SECTRACK:1017433
URL:http://securitytracker.com/id?1017433
SECUNIA:23448
URL:http://secunia.com/advisories/23448

CVE Reference: CVE-2006-6696

❖ 16480 CSRSS Local Elevation of Privilege Vulnerability (MS07-021/930178) (Remote File Checking)

A privilege elevation vulnerability exists in the way that the Windows 32 Client/Server Run-time Subsystem (CSRSS) handles its connections during the startup and stopping of processes.

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

References:

Original advisory:
MS07-021
http://www.microsoft.com/technet/security/bulletin/ms07-021.mspx

Other references:
* BUGTRAQ:20070410 EEYE: Windows Vista CSRSS Dangling Process Pointer Privilege Escalation
* URL:http://www.securityfocus.com/archive/1/archive/1/465233/100/0/threaded

CVE Reference: CVE-2007-1209

❖ 16481 CSRSS DoS Vulnerability (MS07-021/930178) (Remote File Checking)

A denial of service vulnerability exists in the Client/Server Run-time Subsystem (CSRSS) service because of the way it handles error messages. An attacker could exploit the vulnerability by running a specially crafted application causing the system to restart.

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

References:

Original advisory:
MS07-021
http://www.microsoft.com/technet/security/bulletin/ms07-021.mspx

Other references:
BUGTRAQ:20061227 NtRaiseHardError Csrss.exe memory Disclosure exploit
URL:http://www.securityfocus.com/archive/1/archive/1/455365/100/0/threaded
MISC:
http://www.reversemode.com/index.php?option=com_content&task=view&id=29&Itemid=2
MISC:
http://www.reversemode.com/index.php?option=com_remository&Itemid=2&func=fileinfo&id=43
FRSIRT:ADV-2006-5197
URL:http://www.frsirt.com/english/advisories/2006/5197
SECTRACK:1017454
URL:http://securitytracker.com/id?1017454
SECUNIA:23491
URL:http://secunia.com/advisories/23491
XF:win-ntraiseharderror-information-disclosure(31176)
URL:http://xforce.iss.net/xforce/xfdb/31176

CVE Reference: CVE-2006-6797

❖ 16482 Vulnerability in Windows Kernel Could Allow Elevation of Privilege (MS07-022/931784) (Remote File Checking)

A privilege elevation vulnerability exists in Windows Kernel because of incorrect permissions on a mapped memory segment. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

References:

Original advisory:

MS07-022
http://www.microsoft.com/technet/security/bulletin/ms07-022.mspx

CVE Reference: CVE-2007-1206

❖ 17747 PHP "readwbmp()" Integer Overflow Vulnerability

Ivan Fratric has reported a vulnerability in PHP, which potentially can be exploited by malicious people to cause a DoS (Denial of Service) or execute arbitrary code.

The vulnerability is caused due to an integer overflow within the "readwbmp()" function in ext/gd/libgd/wbmp.c. This can be exploited to e.g. cause a DoS by tricking a PHP script into loading a specially crafted wbmp image.

PHP versions 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 are vulnerable to the issue.

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

References:

Original advisory:
http://ifsec.blogspot.com/2007/04/php-521-wbmp-file-handling-integer.html

Other references:
BUGTRAQ:20070407 PHP <= 5.2.1 wbmp file handling integer overflow
URL:http://www.securityfocus.com/archive/1/archive/1/464957/100/0/threaded
MISC: http://cvs.php.net/viewvc.cgi/php-src/ext/gd/libgd/wbmp.c?r1=1.2.4.1&r2=1.2.4.1.8.1
CONFIRM: http://cvs.php.net/viewvc.cgi/php-src/ext/gd/libgd/wbmp.c?revision=1.2.4.1.8.1&view=markup
BID:23357
URL:http://www.securityfocus.com/bid/23357
FRSIRT:ADV-2007-1269
URL:http://www.frsirt.com/english/advisories/2007/1269
XF:php-gd-overflow(33453)
URL:http://xforce.iss.net/xforce/xfdb/33453

CVE Reference: CVE-2007-1001

❖ 17748 PHP "FILTER_VALIDATE_EMAIL" Filter Newline Injection

Stefan Esser has reported a vulnerability in PHP, which can be exploited by malicious people to bypass certain security restrictions.

The vulnerability is caused due to the use of an incorrect regular expression within the "FILTER_VALIDATE_EMAIL" filter of the ext/filter extension. This can be exploited to inject newlines via specially crafted email addresses, which may allow mail header injection.

The vulnerability is reported in PHP 5.2.0 and 5.2.1. 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/PMOPB-45-2007.html

Other references:
BID:23359
URL:http://www.securityfocus.com/bid/23359
SECUNIA:24824
URL:http://secunia.com/advisories/24824

CVE Reference: CVE-2007-1900

❖ 17749 PHP "str_replace()" function, off-by-one Vulnerability

An off-by-one error exists in the "str_replace()" function when replacing one character with another character.

The affected versions of PHP are PHP 4 < 4.4.5 and PHP 5 < 5.2.1.

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

References:

Original advisory:
http://www.php-security.org/MOPB/MOPB-39-2007.html

Other references:
http://secunia.com/advisories/24630/

CVE Reference: CVE-2007-1886

❖ 17750 PHP "unserialize()" function, Information Disclosure Vulnerability

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

An error exists 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 affected versions of PHP are 5.2.1.

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

References:

Original advisory:
http://www.php-security.org/MOPB/MOPB-29-2007.html

Other references:

BID:23105
URL:http://www.securityfocus.com/bid/23105
SECUNIA:24630
URL:http://secunia.com/advisories/24630
XF:php-unserialize-information-disclosure(33170)
URL:http://xforce.iss.net/xforce/xfdb/33170

CVE Reference: CVE-2007-1649

New Vulnerabilities found this Week

Microsoft Agent URL Parsing Memory Corruption Vulnerability
"Execution of arbitrary code"

Secunia Research has discovered a vulnerability in Microsoft Windows, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an error in Microsoft Agent (agentdpv.dll) when processing specially crafted URLs passed as arguments to certain methods.

Successful exploitation allows execution of arbitrary code when a user e.g. visits a malicious website with Internet Explorer.

References:
http://www.microsoft.com/technet/security/Bulletin/MS07-020.mspx
http://descriptions.securescout.com/tc/16478

PHP "readwbmp()" Integer Overflow Vulnerability
"Denial of Service"

Ivan Fratric has reported a vulnerability in PHP, which potentially can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an integer overflow within the "readwbmp()" function in ext/gd/libgd/wbmp.c. This can be exploited to e.g. cause a DoS by tricking a PHP script into loading a specially crafted wbmp image.

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

References:
http://ifsec.blogspot.com/2007/04/php-521-wbmp-file-handling-integer.html
http://descriptions.securescout.com/tc/17747

IPsec Tools "isakmp_inf.c" Denial of Service
"Denial of Service"

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

The vulnerability is caused due to an error within src/racoon/isakmp_inf.c. This can be

exploited to e.g. interrupt existing IPSec tunnels by sending a specially crafted packet.

The vulnerability is reported in versions prior to 0.6.7.

References:
http://sourceforge.net/mailarchive/message.php?msg_name=20070406123739.GA1546%40zen.inc

Linux Kernel "atalk_sum_skb()" AppleTalk Denial of Service
"Denial of Service"

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

The vulnerability is caused due to an error within the "atalk_sum_skb()" function when creating the checksum of an AppleTalk frame that is shorter than specified in the header. This can be exploited to trigger a "BUG_ON" condition by sending a specially crafted AppleTalk frame to a vulnerable system.

Successful exploitation requires that the AppleTalk kernel module is loaded.

References:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.20.5
http://bugzilla.kernel.org/show_bug.cgi?id=2979

PHP "FILTER_VALIDATE_EMAIL" Filter Newline Injection
"Mail header injection"

Stefan Esser has reported a vulnerability in PHP, which can be exploited by malicious people to bypass certain security restrictions.

The vulnerability is caused due to the use of an incorrect regular expression within the "FILTER_VALIDATE_EMAIL" filter of the ext/filter extension. This can be exploited to inject newlines via specially crafted email addresses, which may allow mail header injection.

The vulnerability is reported in PHP 5.2.0 and 5.2.1. Other versions may also be affected.

References:
http://www.php-security.org/MOPB/PMOPB-45-2007.html
http://descriptions.securescout.com/tc/17748

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