

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

[Task Scheduler Vulnerability Scanner](#) – The Task Scheduler Vulnerability 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 Task Scheduler flaw (MS04-022).

This Week in Review

Privacy group tries to stop Google. Companies increasingly concerned over Wi-Fi security. Next spending-spree: Australia. Hurdles when researching security.

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

❖ Privacy groups ask FTC to block Google-DoubleClick merger

Three U.S. online civil rights groups have filed a complaint asking the U.S. Federal Trade Commission (FTC) to block Google Inc.'s planned \$3.1 billion acquisition of DoubleClick Inc. unless the company agrees to stop tracking its users.

The complaint, filed today by the Electronic Privacy Information Center (EPIC), the Center for Digital Democracy (CDD) and the U.S. Public Interest Research Group (US

PIRG), calls upon the FTC to block the merger unless it obtains guarantees from Google and DoubleClick that they will protect Internet users' privacy.

Those guarantees include a promise to destroy all cookies and other persistent identifiers resulting from Internet searches that are or could be personally identifiable once a user terminates a session with Google.

Such a move would seriously affect many of the services Google offers, which are built on storing the entire search or transaction history of its users.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9017298&taxonomyId=17&intsrc=kc_top

❖ **Concerns grow over rogue Wi-Fi security**

Rogue and insecure Wi-Fi access points are increasingly posing a threat to the security of corporate networks.

One of the main worries about wireless security is users unwittingly accessing insecure or malicious wireless networks when they are out of the office, according to a survey this week. And 10 out of the 12-strong CIO Jury IT user panel, organised by ZDnet UK's sister site silicon.com, agreed that Wi-Fi security is a major concern.

Gavin Whatrup, group IT director at marketing services company Creston, said his organisation has taken the decision not to install a wireless infrastructure until the security elements of Wi-Fi have matured.

zdnet

Full Story :

<http://news.zdnet.co.uk/communications/0,1000000085,39286782,00.htm>

❖ **Australia set for huge spending spree on security**

In-house developed and managed security software will face extinction, says IDC. The Australian security software market is set to rise a staggering 65% by 2010, as vendors continue to binge on acquisitions to provide more bundled offerings, and users beef-up security infrastructure to combat new threats.

IDC's security system management analyst, Patrik Bihammar, says the local security market will increase from A\$850 million to A\$1.3 billion in less than three years.

Bihammar says security software will maintain its annual compound growth rate of 13.4%, well ahead of other software markets.

His assessment of the local market and emerging trends through to 2010 will be presented at IDC's security and continuity conference which will be held in Sydney on Tuesday.

computerworld

Full Story :

<http://computerworld.co.nz/news.nsf/news/0D9FAD9DEBB072ACCC2572C3001C31AC>

❖ Security researchers face hurdles

Security researchers say that they are still facing hurdles in developing solutions for the latest security attacks.

In one example from last year, US security expert Cody Pierce of Tipping Point thought the he knew right away what he had found, but he wasn't exactly sure how serious it was. Pierce and his fellow researchers had spent much of the early part of last year poking around in the ActiveX controls in Windows XP, looking for controls that might be vulnerable.

The team had decided at the beginning of the year that with all of the applications and code now running on the Web instead of desktops, ActiveX would be a prime avenue of attack for hackers in the coming months and years, and they wanted to get there before the attackers did.

Computerweekly.com

Full Story :

<http://www.computerweekly.com/Articles/2007/04/20/223344/security-researchers-face-hurdles.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.msp>

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.msp>

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.msp>

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](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](http://www.securityfocus.com/archive/1/archive/1/455104/100/0/threaded)

BUGTRAQ:20061221 Re: [Full-disclosure] Microsoft Windows XP/2003/Vista memory corruption 0day
#

[URL:http://www.securityfocus.com/archive/1/archive/1/455088/100/0/threaded](http://www.securityfocus.com/archive/1/archive/1/455088/100/0/threaded)

BUGTRAQ:20061222 Re: [Full-disclosure] Microsoft Windows XP/2003/Vista memory corruption 0day
#

[URL:http://www.securityfocus.com/archive/1/archive/1/455158/100/0/threaded](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/csrs-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>

MILWORM: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.msp>

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.msp>

Other references:

BUGTRAQ:20061227 NtRaiseHardError Csrss.exe memory Disclosure exploit

[URL:http://www.securityfocus.com/archive/1/archive/1/455365/100/0/threaded](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=filinfo&id=43

FRSIRT:ADV-2006-5197

[URL:http://www.frsirt.com/english/advisories/2006/5197](http://www.frsirt.com/english/advisories/2006/5197)

SECTRACK:1017454

[URL:http://securitytracker.com/id?1017454](http://securitytracker.com/id?1017454)

SECUNIA:23491

[URL:http://secunia.com/advisories/23491](http://secunia.com/advisories/23491)

XF:win-ntraiseharderror-information-disclosure(31176)

[URL:http://xforce.iss.net/xforce/xfdb/31176](http://xforce.iss.net/xforce/xfdb/31176)

CVE Reference: [CVE-2006-6797](http://cve.mitre.org/cgi-bin/cvehandler.cgi?id=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.msp>

CVE Reference: [CVE-2007-1206](http://cve.mitre.org/cgi-bin/cvehandler.cgi?id=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](https://cve.mitre.org/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](http://xforce.iss.net/xforce/xfdb/33170)

CVE Reference: [CVE-2007-1649](#)

New Vulnerabilities found this Week

Adobe Photoshop Bitmap File Handling Buffer Overflow Vulnerability

“Execution of arbitrary code”

Marsu has reported a vulnerability in Adobe Photoshop, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an error within the handling of Bitmap files (e.g. .BMP, .DIB, .RLE) and can be exploited to cause a stack-based buffer overflow via a specially crafted Bitmap file.

Successful exploitation allows execution of arbitrary code.

The vulnerability is reported in Adobe Photoshop CS2 and CS3. Other versions may also be affected.

References:

<http://milw0rm.com/exploits/3793>

Apple QuickTime Java Handling Unspecified Code Execution

“Execute arbitrary code”

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

The vulnerability is caused due to an unspecified error within the Java handling in QuickTime. This can be exploited to execute arbitrary code when a user visits a malicious web site using a Java-enabled browser e.g. Safari or Firefox.

The vulnerability is reported on a Mac OS X system using Safari and Firefox. Other browsers and platforms may also be affected.

References:

<http://www.matasano.com/log/812/breaking-macbook-vuln-in-quicktime-affects-win32-apple-code/>

Linksys SPA941 SIP Message Denial of Service

“Denial of Service”

Radu State has reported a vulnerability in the Linksys SPA941 VoIP Phone, 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 messages. This can be exploited to reboot the phone by sending specially crafted SIP messages containing

"\337" characters.

The vulnerability is reported in software version 5.1.5. Other versions may also be affected.

References:

<http://lists.grok.org.uk/pipermail/full-disclosure/2007-April/053959.html>

Linux Kernel "L2CAP" and "HCI" Information Disclosure

"Disclose potential sensitive information"

Two weaknesses have been reported in the Linux Kernel, which can be exploited by malicious, local users to disclose potential sensitive information.

The weaknesses are caused due to uninitialised variables within the "hci_sock_setsockopt()" function in net/bluetooth/hci_sock.c and the "l2cap_sock_setsockopt()" function in net/bluetooth/l2cap.c and can potentially be exploited to disclose uninitialised bytes of the kernel stack.

The weaknesses are reported in versions prior to 2.4.34.3.

References:

<http://kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.34.3>

PostgreSQL SECURITY DEFINER Functions Privilege Escalation

"Gain escalated privileges"

A security issue has been reported in PostgreSQL, which potentially can be exploited by malicious users to gain escalated privileges.

The security issue is caused due to an error in SECURITY DEFINER functions and can be exploited to gain escalated privileges by modifying the search_path and using temporary objects.

References:

<http://www.postgresql.org/about/news.791>

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