netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 32

August 17, 2007

Table of Contents

Product Focus

netVigilance has ported Honeyd 1.5c to Windows, and released it for free under the name WinHoneyd.
The complete source and the compiled executable are available for free on our web-site.
The update from winhoneyd 1.5b to 1.5c is mainly a bugfix /code optimization release.
To download WinHoneyd.exe or the WinHoneyd source please visit
http://www.netvigilance.com/winhoneyd

Mydoom Worm Scanner – The S4 MyDoom Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any have been infected by the MyDoom email virus or its variants.

This Week in Review

Malware increasingly uses a variety of vulnerabilities. Vague PCI guidelines under critisism. Open source credibility maturing. Online safety to become part of curriculum.

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

❖ Malware Evolution: April - June 2007

The events that took place during the first six months of 2007 have shown us that the direction in which threats are evolving is from social engineering to the increased usage of a variety of vulnerabilities to penetrate the system.

The virus writing "crisis of ideas" that we wrote about at the close of last year (and which we feared would end in a crisis in the near future) is still in full swing. The current period is characterized by the lack of any real new threats and an upswing in the commercialization of the virus writing environment. As I previously confirmed, the ball is now in our court - for the first time in many years, the antivirus companies have the upper hand. Virus writers are concerned solely with earning dirty money and are incapable of coming up with new ideas, so instead they are trying to milk what they can out of old technologies - and the antivirus industry is coping quite well. The worst thing about the current situation is that quality has given way to quantity.

Help net security

Full Story :
http://www.net-security.org/article.php?id=1054

❖ Secure miffed at 'vague' PCI regs

A Secure Computing executive has called on the PCI Security Standards Council to clarify what it means when it instructs merchants to deploy 'application firewalls.'

"The standard is too vague," said Secure's vice president of technology evangelism Paul Henry, in an interview.

Henry said the PCI guidelines, which the big five credit card companies are obliging their merchant partners to abide by, should define "application layer firewall" to mean a firewall that "breaks the client-server model".

Not coincidentally, that definition would be met by Secure's longstanding proxy-based firewall products, but perhaps not by rival products from competitors that have their roots in the packet-filter firewall segment.
CBR

Full Story :
http://www.cbronline.com/article_news.asp?guid=E0A29AF4-5147-476B-85A6-3F4937123C39

❖ Open Source Security, Part 1: Securing Credibility

Some quarters in the software industry still carry a bias against the credibility of open source security applications. Open source network gateway developer Untangle did not

expect to find its request for certified testing of the popular open source virus security product ClamAV shunned. When it was, Untangle decided to do its own test.
Open source applications have come into their own. For some time, open source programmers held much the same reputation as shareware authors. They were little more than experimenters and programming geeks who chose the alternate code-writing route because they could not or did not want to compete in the real software industry of commercial programming.

Linuxinsider

Full Story :
http://www.linuxinsider.com/story/DaJf1MgBkn4c4J/Open-Source-Security-Part-1-Securing-Credibility.xhtml l

❖ US curriculum to include online safety

The US National Cyber Security Alliance (NCSA) has called on state leaders to work with schools and colleges to ensure that cyber-security, online safety and ethics lessons are integrated into every classroom.

The call has been made with support from companies including CA, McAfee, Microsoft and Symantec, along with educational organisations such as the Consortium for School Networking and the State Education Technology Directors Association.

Recent legislation dubbed the No Child Left Behind Act requires students to be technology-literate on completion of the eighth grade (year nine in the UK), and the NCSA argues that children should also be taught about the dangers of the web.

vnunet

Full Story :
http://www.vnunet.com/vnunet/news/2196759/ncsa-urges-schools-teach-cyber

New Vulnerabilities Tested in SecureScout

❖ 16583 Windows Media Player Code Execution Vulnerability Decompressing Skins (MS07-047/936782) (Remote File Checking)

A remote code execution vulnerability exists in Windows Media Player 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:

References:

* MS: MS07-047
http://www.microsoft.com/technet/security/bulletin/ms07-047.mspx
* MISC:
http://www.zerodayinitiative.com/advisories/ZDI-07-047.html
* SECTRACK: 1018565
http://securitytracker.com/id?1018565

CVE Reference: CVE-2007-3891

❖ 16582 Windows Media Player Code Execution Vulnerability Parsing Skins (MS07-047/936782) (Remote File Checking)

A code execution vulnerability exists in Windows Media Player skin parsing. 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:

* MS: MS07-047
http://www.microsoft.com/technet/security/bulletin/ms07-047.mspx
* MISC:
http://www.zerodayinitiative.com/advisories/ZDI-07-046.html
* SECTRACK: 1018565
http://securitytracker.com/id?1018565

CVE Reference: CVE-2007-3032

❖ 16581 VML Buffer Overrun Vulnerability (MS07-050/938127) (Remote File Checking)

A remote code execution vulnerability exists in the Vector Markup Language (VML) implementation in Microsoft Windows. An attacker could exploit the vulnerability by constructing a specially crafted Web page or HTML e-mail. When a user views the Web page or the message, the vulnerability could allow remote code execution.

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

References:

* BUGTRAQ: 20070814 EEYE: VGX.DLL Compressed Content Heap Overflow Vulnerability
http://www.securityfocus.com/archive/1/archive/1/476498/100/0/threaded
* MISC:
http://research.eeye.com/html/advisories/published/AD20070814a.html
* MS: MS07-050
http://www.microsoft.com/technet/security/bulletin/ms07-050.mspx

* CERT-VN: VU#468800
http://www.kb.cert.org/vuls/id/468800
* BID: 25310
http://www.securityfocus.com/bid/25310
* SECTRACK: 1018568
http://www.securitytracker.com/id?1018568
* SECUNIA: 26409
http://secunia.com/advisories/26409

CVE Reference: CVE-2007-1749

❖ 16580 Remote Code Execution Vulnerability in GDI (MS07-046/938829) (Remote File Checking)

A remote code execution vulnerability exists in the Graphics Rendering Engine because of the way that it handles specially crafted images. An attacker could exploit the vulnerability by constructing a specially crafted image that could potentially allow remote code execution if a user opened a specially crafted attachment in e-mail.

An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* MS: MS07-046
http://www.microsoft.com/technet/security/bulletin/ms07-046.mspx
* CERT-VN: VU#640136
http://www.kb.cert.org/vuls/id/640136
* BID: 25302
http://www.securityfocus.com/bid/25302
* SECTRACK: 1018563
http://www.securitytracker.com/id?1018563
* SECUNIA: 26423
http://secunia.com/advisories/26423

CVE Reference: CVE-2007-3034

❖ 16579 Internet Explorer, ActiveX Object Memory Corruption Vulnerability (MS07-045/937143) (Remote File Checking)

A remote code execution vulnerability exists in the ActiveX object, pdwizard.ocx. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user.

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

References:

* MS: MS07-045
http://www.microsoft.com/technet/security/bulletin/ms07-045.mspx

CVE Reference: CVE-2007-3041

❖ 16578 Internet Explorer, ActiveX Object Vulnerability (MS07-045/937143) (Remote File Checking)

ucting a specially crafted Web page that could potentially allow remote code execution if a user visited the Web page. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user.

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

References:

* MS: MS07-045
http://www.microsoft.com/technet/security/bulletin/ms07-045.mspx

CVE Reference: CVE-2007-2216

❖ 16577 Internet Explorer, CSS Memory Corruption Vulnerability (MS07-045/937143) (Remote File Checking)

A remote code execution vulnerability exists in the way Internet Explorer parses certain strings in CSS. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user.

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

References:

* MS: MS07-045
http://www.microsoft.com/technet/security/bulletin/ms07-045.mspx

CVE Reference: CVE-2007-0943

❖ 16576 Microsoft Excel Workspace Memory Corruption Vulnerability (MS07-044/940965) (Remote File Checking)

A remote code execution vulnerability exists in the way Excel handles malformed Excel files. An attacker could exploit the vulnerability by sending a malformed file which could be included as an e-mail attachment, or hosted on a malicious or compromised Web site.

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

References:

* MS: MS07-044
http://www.microsoft.com/technet/security/bulletin/ms07-044.mspx
* BID: 25280
http://www.securityfocus.com/bid/25280
* SECTRACK: 1018561
http://www.securitytracker.com/id?1018561
* SECUNIA: 26145
http://secunia.com/advisories/26145

CVE Reference: CVE-2007-3890

❖ 16575 OLE Automation Memory Corruption Vulnerability (MS07-043/921503) (Remote File Checking)

A remote code execution vulnerability exists in Object linking and embedding (OLE) Automation that could allow an attacker who successfully exploited this vulnerability to make changes to the system with the permissions of the logged-on user. If a user is logged on with administrative user rights, an attacker could take complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* BUGTRAQ: 20070814 ZDI-07-048: Microsoft Internet Explorer substringData() Heap Overflow Vulnerability
http://www.securityfocus.com/archive/1/archive/1/476527/100/0/threaded
* MS: MS07-043
http://www.microsoft.com/technet/security/bulletin/ms07-043.mspx
* BID: 25282
http://www.securityfocus.com/bid/25282
* SECTRACK: 1018560
http://www.securitytracker.com/id?1018560

* SECUNIA: 26449
http://secunia.com/advisories/26449

CVE Reference: CVE-2007-2224

❖ 16574 Microsoft XML Core Services Vulnerability (MS07-042/936227) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft XML Core Services that could allow an attacker who successfully exploited this vulnerability to make changes to the system with the permissions of the logged-on user. If a user is logged on with administrative user rights, an attacker could take complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* BUGTRAQ: 20070814 ZDI-07-048: Microsoft Internet Explorer substringData() Heap Overflow Vulnerability
http://www.securityfocus.com/archive/1/archive/1/476527/100/0/threaded
* MS: MS07-042
http://www.microsoft.com/technet/security/bulletin/ms07-042.mspx
* CERT-VN: VU#361968
http://www.kb.cert.org/vuls/id/361968
* BID: 25301
http://www.securityfocus.com/bid/25301
* FRSIRT: ADV-2007-2866
http://www.frsirt.com/english/advisories/2007/2866
* SECTRACK: 1018559
http://www.securitytracker.com/id?1018559
* SECUNIA: 26447
http://secunia.com/advisories/26447

CVE Reference: CVE-2007-2223

New Vulnerabilities found this Week

Microsoft Patch Tuesday August 2007

"Denial of service; Code execution; Information disclosure"

This past Tuesday, Microsoft released patches for many of its products.

VML Buffer Overrun Vulnerability (MS07-050/938127)

Windows Media Player Code Execution Vulnerability Parsing Skins (MS07-047/936782)
Windows Media Player Code Execution Vulnerability Decompressing Skins (MS07-047/936782)
Virtual PC and Virtual Server Heap Overflow Vulnerability (MS07-049/937986)
Microsoft XML Core Services Vulnerability (MS07-042/936227)
OLE Automation Memory Corruption Vulnerability (MS07-043/921503)
Microsoft Excel Workspace Memory Corruption Vulnerability (MS07-044/940965)
Internet Explorer, CSS Memory Corruption Vulnerability (MS07-045/937143)
Internet Explorer, ActiveX Object Vulnerability (MS07-045/937143)
Internet Explorer, ActiveX Object Memory Corruption Vulnerability (MS07-045/937143)
Remote Code Execution Vulnerability in GDI (MS07-046/938829)
Windows Vista Feed Headlines Gadget Could Allow Remote Code Execution (MS07-048/938123)
Windows Vista Contacts Gadget Could Allow Code Execution (MS07-048/938123)
Windows Vista Weather Gadget Could Allow Remote Code Execution (MS07-048/938123)

References:
http://www.microsoft.com/technet/security/Bulletin/ms07-042.mspx
http://www.microsoft.com/technet/security/Bulletin/ms07-043.mspx
http://www.microsoft.com/technet/security/Bulletin/ms07-044.mspx
http://www.microsoft.com/technet/security/Bulletin/ms07-045.mspx
http://www.microsoft.com/technet/security/Bulletin/ms07-046.mspx
http://www.microsoft.com/technet/security/Bulletin/ms07-047.mspx
http://www.microsoft.com/technet/security/Bulletin/ms07-048.mspx
http://www.microsoft.com/technet/security/Bulletin/ms07-049.mspx
http://www.microsoft.com/technet/security/Bulletin/ms07-050.mspx
http://descriptions.securescout.com/tc/16574
http://descriptions.securescout.com/tc/16575
http://descriptions.securescout.com/tc/16576
http://descriptions.securescout.com/tc/16577
http://descriptions.securescout.com/tc/16578
http://descriptions.securescout.com/tc/16579
http://descriptions.securescout.com/tc/16580
http://descriptions.securescout.com/tc/16581
http://descriptions.securescout.com/tc/16582
http://descriptions.securescout.com/tc/16583
http://descriptions.securescout.com/tc/16584
http://descriptions.securescout.com/tc/16585
http://descriptions.securescout.com/tc/16586
http://descriptions.securescout.com/tc/16587

Opera JavaScript Invalid Pointer Vulnerability

“Execute arbitrary code”

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

The vulnerability is caused due to an unspecified error when processing JavaScript code and can result in a virtual function call using an invalid pointer. This can be exploited to execute arbitrary code by e.g. tricking a user into visiting a malicious website.

The vulnerability is reported in versions prior to 9.23.

References:
http://www.opera.com/support/search/view/865/

Cisco VPN Client Privilege Escalation Vulnerabilities

“Gain escalated privileges”

Some vulnerabilities have been reported in Cisco VPN Client, which can be exploited by malicious, local users to gain escalated privileges.

1) An error when using a VPN profile configured to use the Microsoft Dial-Up Networking Interface can be exploited to run arbitrary commands with the privileges of the LocalSystem account by enabling the "Start Before Logon" feature.

The vulnerability is reported in versions prior to 4.8.02.0010.

2) Incorrect permissions are set for cpvnd.exe during the Cisco VPN Client installation. This can be exploited by interactive users to run arbitary commands with the privileges of the LocalSystem account by replacing cvpnd.exe with an arbitrary file.

The vulnerability is reported in versions prior to 5.0.01.0600.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20070815-vpnclient.shtml

Sun JRE Font Parsing Vulnerability

“Execute local applications”

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

The vulnerability is caused due to an unspecified error in the parsing of fonts contained in Java applets. This can be exploited by malicious, untrusted applets to read and write local files, or to execute local applications.

The vulnerability is reported in the following products:
* JDK and JRE 5.0 Update 9 and earlier
* SDK and JRE 1.4.2_14 and earlier

SDK and JRE 1.3.1_xx are not affected by the vulnerability.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-103024-1

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