netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 24

June 16, 2006

Table of Contents

Product Focus

ASN.1 Vulnerability Scanner – The Apache Chunked 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 Apache Chunked Encoding buffer overflow.

This Week in Review

Bots steal pay-per-click, Payable QoS on Internet gets backing in Senate, Porn Surfing Oregon Tax man downloads Trojan at work.

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

- **Web Ads Present New Front In Hacker Wars**

THE RISE OF "pay-per-click" online advertising, celebrated for turning Google Inc. and Yahoo Inc. into enormous businesses, is proving a boon for cyberthieves.

Hackers are using increasingly sophisticated computer programs to automate phony clicks on Internet ads and then hide the click fraud from detection. This threat, though still small, poses a challenge for Google, Yahoo and other Internet companies that sell pay-per-click ads and need to assure advertisers that they are paying for legitimate clicks from potential customers.

A catalyst has been the explosion of "bots" -- malicious software that hackers sneak onto thousands of home computers and network together into huge "botnets." The click-fraud programs can be changed quickly, making it easier for them to evade security software and to be customized for different fraud schemes.

Botnets are most commonly used to attack and shut down Web sites with floods of bogus traffic, often as part of extortion schemes, or to steal personal information for use in identity-theft scams.

Dowjones Newswires

Full Story :
http://framehosting.dowjonesnews.com/sample/samplestory.asp?StoryID=2006061423550000&Take=1

❖ Senate Showing Little Interest in Net Neutrality

WASHINGTON - The network neutrality debate resumed today in the U.S. Senate the way it ended in the House of Representatives Thursday night: apparently dead on arrival.

As the Senate Commerce Committee held its third of three hearings on a telecom reform bill, lawmakers seemed content to leave the controversial issue to the Federal Communications Commission (FCC).

"We do already have [network neutrality] principles set forward by the FCC," Sen. John Sununu (R-N.H.) said. "The House legislation steers in the right direction."

Last week, the House passed telecom reform legislation that features national video franchising and a clause that empowers the FCC to enforce the network neutrality principles the agency approved last August.

The FCC principles would allow broadband providers such as AT&T and Comcast to create a two-tiered Internet with extra fees charged to bandwidth-intensive content providers like Google, Yahoo and Amazon.

Internetnews.com

Full Story :

http://www.internetnews.com/bus-news/article.php/3613186

❖ Porn-surfing hits taxpayer IDs

Security breach - More than 1,300 people face identity theft after a state employee let in data-stealing spyware.

Oregon Department of Revenue officials thought they were tightly secured against data theft. An elaborate firewall around their computer system fended off hackers. Virus detection software, updated every two hours, constantly screened incoming e-mail and downloads for malicious programs.

But the technology did not stop an employee from using an office computer to surf porn sites and download a Trojan horse, a hidden spyware program not yet known to intrusion-detection software. The Trojan installed itself Jan. 5 and for the next four months secretly captured and relayed data to the hackers who created it.

More than 1,300 taxpayers are now at risk of identity theft. The Department of Revenue, which disclosed the security breach Tuesday, said the confidential data consisted of Social Security numbers, names and addresses but included no tax records or financial or credit card information.
Oregonian

Full Story :
http://www.oregonlive.com/news/oregonian/index.ssf?/base/news/1150253715120440.xml&coll=7

New Vulnerabilities Tested in SecureScout

❖ **16264 Cumulative Security Update for Internet Explorer (MS06-021/916281) (Remote File Checking)**

A remote code execution vulnerability exists in the way Internet Explorer handles exceptional conditions. As a result, system memory may be corrupted in such a way that an attacker could execute arbitrary code if a user visited a specially crafted Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

A remote code execution vulnerability exists in the way Internet Explorer decodes specially crafted UTF-8 encoded HTML. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code execution if a user visited the specially crafted Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

A remote code execution vulnerability exists in the DXImageTransform.Microsoft.Light ActiveX control if passed unexpected data. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code execution if a user visited the specially crafted Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

A remote code execution vulnerability exists in the way Internet Explorer instantiates COM objects that are not intended to be instantiated in Internet Explorer. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code execution if a user visited the specially crafted Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

An information disclosure vulnerability exists in Internet Explorer because it incorrectly interprets a specially crafted document as a cascading style sheet (CSS). An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially lead to information disclosure if a user visited a specially crafted Web site or clicked a link in a specially crafted e-mail message. An attacker who successfully exploited this vulnerability could read file data from another Internet Explorer domain. However, user interaction is required to exploit this vulnerability.

A spoofing vulnerability exists in Internet Explorer that could allow an attacker to display spoofed content in a browser window. The address bar and other parts of the trust UI can be displayed from trusted Web sites but the content of the window contains the attacker's Web page.

A remote code execution vulnerability exists in the way Internet Explorer saves multipart HTML (.mht) files. An attacker could exploit the vulnerability by constructing a specially crafted Web page and convince a user to save this Web page as a multipart HTML file that could potentially allow remote code execution. An attacker who successfully exploited this vulnerability could take complete control of an affected system however significant user interaction is required.

A spoofing vulnerability exists in Internet Explorer that could allow an attacker to display spoofed content in a browser window. The address bar and other parts of the trust UI can be displayed from trusted Web sites but the content of the window contains the attacker's Web page.

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

References:

Original advisory:
MS06-021
http://www.microsoft.com/technet/security/bulletin/ms06-021.mspx

Product HomePage:
http://www.microsoft.com/windows/ie

CVE Reference:
CVE-2006-2218
CVE-2006-2382
CVE-2006-2383
CVE-2006-1303
CVE-2005-4089
CVE-2006-2384
CVE-2006-2385
CVE-2006-1626

❖ 16265 Vulnerability in ART Image Rendering Could Allow Remote Code Execution (MS06-022/918439) (Remote File Checking)

There is a remote code execution vulnerability in the way that Windows handles ART images. An attacker could exploit the vulnerability by constructing a specially crafted ART image that could potentially allow remote code execution if a user visited a Web site or viewed a specially crafted e-mail message. 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:
* IDEFENSE:20060613 Microsoft Internet Explorer ART File Heap Corruption Vulnerability
http://www.idefense.com/intelligence/vulnerabilities/display.php?id=407
* MS06-022
http://www.microsoft.com/technet/security/bulletin/ms06-022.mspx

Other references:
* CERT-VN:VU#923236
* URL:http://www.kb.cert.org/vuls/id/923236
* BID:18394
* URL:http://www.securityfocus.com/bid/18394
* FRSIRT:ADV-2006-2320
* URL:http://www.frsirt.com/english/advisories/2006/2320
* SECUNIA:20605
* URL:http://secunia.com/advisories/20605

CVE Reference:
CVE-2006-2378

❖ 16266 Vulnerability in Microsoft JScript Could Allow Remote Code Execution (MS06-023/917344) (Remote File Checking)

There is a remote code execution vulnerability in JScript. An attacker could exploit the vulnerability by constructing specially crafted JScript that could potentially allow remote code execution if a user visited a Web site or viewed a specially crafted e-mail message. 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:
MS06-023
http://www.microsoft.com/technet/security/bulletin/ms06-023.mspx

Other references:
# CERT-VN:VU#390044
# URL:http://www.kb.cert.org/vuls/id/390044
# BID:18359
# URL:http://www.securityfocus.com/bid/18359
# FRSIRT:ADV-2006-2321
# URL:http://www.frsirt.com/english/advisories/2006/2321
# SECUNIA:20620
# URL:http://secunia.com/advisories/20620

CVE Reference: CVE-2006-1313

❖ 14721 Mozilla Firefox "nsHTMLContentSink.cpp", memory corruption Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

An error in the processing of a certain sequence of HTML tags in "nsHTMLContentSink.cpp" can be exploited to cause a memory corruption.

Successful exploitation allows execution of arbitrary code.

The vulnerability has been reported in version 1.0 and 1.5.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2006/mfsa2006-18.html

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2006-0749

❖ 16267 Vulnerability in Windows Media Player Could Allow Remote Code Execution (MS06-024/917734) (Remote File Checking)

A remote code execution vulnerability exists in Windows Media Player due to the way it handles the processing of PNG images. An attacker could exploit the vulnerability by constructing specially crafted Windows Media Player content that could potentially allow remote code execution if a user visits a malicious Web site or opens an email message with malicious content. 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:
* IDEFENSE:20060613 Windows Media Player PNG Chunk Decoding Stack-Based Buffer Overflow
http://www.idefense.com/intelligence/vulnerabilities/display.php?id=406
* MS06-024
http://www.microsoft.com/technet/security/bulletin/ms06-024.mspx

Other references:
* BID:18385
* URL:http://www.securityfocus.com/bid/18385
* FRSIRT:ADV-2006-2322
* URL:http://www.frsirt.com/english/advisories/2006/2322
* SECUNIA:20626
* URL:http://secunia.com/advisories/20626

CVE Reference: CVE-2006-0025

❖ 16268 Vulnerability in Routing and Remote Access Could Allow Remote Code Execution (MS06-025/911280) (Remote File Checking)

There is a remote code execution vulnerability in the Routing and Remote Access Service that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

There is a remote code execution vulnerability in the Routing and Remote Access Service that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

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

References:
Original advisory:
* MS06-025
http://www.microsoft.com/technet/security/bulletin/ms06-025.mspx

Other references:
* BID:18325
* URL:http://www.securityfocus.com/bid/18325
* FRSIRT:ADV-2006-2323
* URL:http://www.frsirt.com/english/advisories/2006/2323

CVE Reference:
CVE-2006-2370
CVE-2006-6371

❖ 16270 Vulnerability in Microsoft Word Could Allow Remote Code Execution (MS06-027/917336) (Remote File Checking)

A remote code execution vulnerability exists in Word using a malformed object pointer. An attacker could exploit the vulnerability by constructing a specially crafted Word file that could allow remote code execution.

If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an 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 affected than users who operate with administrative user rights.

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

References:

Original advisory:
* MS06-027
http://www.microsoft.com/technet/security/bulletin/ms06-027.mspx

Other references:
* MISC: http://isc.sans.org/diary.php?storyid=1345
* MISC: http://isc.sans.org/diary.php?storyid=1346
* MISC: http://blogs.technet.com/msrc/archive/2006/05/19/429353.aspx
* CONFIRM: http://www.microsoft.com/technet/security/advisory/919637.mspx
* CERT:TA06-139A
* URL: http://www.us-cert.gov/cas/techalerts/TA06-139A.html
* CERT-VN:VU#446012
* URL:http://www.kb.cert.org/vuls/id/446012
* BID:18037
* URL:http://www.securityfocus.com/bid/18037
* FRSIRT:ADV-2006-1872
* URL:http://www.frsirt.com/english/advisories/2006/1872
* OSVDB:25635
* URL:http://www.osvdb.org/25635
* SECTRACK:1016130
* URL:http://securitytracker.com/id?1016130
* SECUNIA:20153
* URL:http://secunia.com/advisories/20153
* XF:word-code-execution(26556)
* URL:http://xforce.iss.net/xforce/xfdb/26556

CVE Reference: CVE-2006-2492

❖ 16271 Vulnerability in Microsoft PowerPoint Could Allow Remote Code Execution (MS06-028/916768) (Remote File Checking)

There is a remote code execution vulnerability in PowerPoint that uses a malformed record. An attacker could exploit the vulnerability by constructing a specially crafted PowerPoint file that could allow remote code execution.

If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an 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 affected than users who operate with administrative user rights.

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

References:

Original advisory:
* MS06-028
http://www.microsoft.com/technet/security/bulletin/ms06-028.mspx

Other references:
* CERT-VN:VU#190089
* URL:http://www.kb.cert.org/vuls/id/190089
* BID:18382
* URL:http://www.securityfocus.com/bid/18382
* FRSIRT:ADV-2006-2325
* URL:http://www.frsirt.com/english/advisories/2006/2325

* SECUNIA:20633
* URL:http://secunia.com/advisories/20633

CVE Reference: CVE-2006-0022

❖ 16272 Vulnerability in Microsoft Exchange Server Running Outlook Web Access Could Allow Script Injection (MS06-029/912442) (Remote File Checking)

A script injection vulnerability exists in Exchange Server running Outlook Web Access (OWA). An attacker could exploit the vulnerability by constructing an e-mail message with a specially crafted script. If this specially crafted script is run, it would execute in the security context of the user on the client. Attempts to exploit this vulnerability require user interaction.

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

References:

Original advisory:
* MS06-029
http://www.microsoft.com/technet/security/bulletin/ms06-029.mspx

Other references:
* BID:18381
* URL:http://www.securityfocus.com/bid/18381
* FRSIRT:ADV-2006-2326
* URL:http://www.frsirt.com/english/advisories/2006/2326

CVE Reference: CVE-2006-1193

❖ 16273 Vulnerability in Server Message Block Could Allow Elevation of Privilege (MS06-030/914389) (Remote File Checking)

There is an elevation of privilege vulnerability in Server Message Block (SMB) that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

There is denial of service vulnerability in Server Message Block (SMB) that could allow an attacker who successfully exploited this vulnerability to cause an affected system to stop responding.

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

References:

Original advisory:
* MS06-030
http://www.microsoft.com/technet/security/bulletin/ms06-030.mspx

Other references:

* IDEFENSE:20060613 Windows MRXSMB.SYS MRxSmbCscIoctlOpenForCopyChunk Overflow
* URL:http://www.idefense.com/intelligence/vulnerabilities/display.php?id=408
* BID:18356
* URL:http://www.securityfocus.com/bid/18356
* FRSIRT:ADV-2006-2327
* URL:http://www.frsirt.com/english/advisories/2006/2327
* IDEFENSE:20060613 Windows MRXSMB.SYS MrxSmbCscIoctlCloseForCopyChunk DoS
* URL:http://www.idefense.com/intelligence/vulnerabilities/display.php?id=409
* BID:18357
* URL:http://www.securityfocus.com/bid/18357

CVE Reference: CVE-2006-2373

❖ 16274 Vulnerability in RPC Mutual Authentication Could Allow Spoofing (MS06-031/917736) (Remote File Checking)

There is a spoofing vulnerability in the way that RPC handles mutual authentication. This vulnerability could allow an attacker to persuade a user to connect to a malicious RPC server which appears to be valid.

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

References:

Original advisory:
* MS06-031
http://www.microsoft.com/technet/security/bulletin/ms06-031.mspx

Other references:
* BID:18389
* URL:http://www.securityfocus.com/bid/18389
* FRSIRT:ADV-2006-2328
* URL:http://www.frsirt.com/english/advisories/2006/2328

CVE Reference: CVE-2006-2380

❖ 16275 Vulnerability in TCP/IP Could Allow Remote Code Execution (MS06-032/917953) (Remote File Checking)

There is a remote code execution vulnerability in the TCP/IP Protocol driver that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

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

References:

Original advisory:
* MS06-032
http://www.microsoft.com/technet/security/bulletin/ms06-032.mspx

Other references:

* CERT-VN:VU#722753
* URL:http://www.kb.cert.org/vuls/id/722753
* BID:18374
* URL:http://www.securityfocus.com/bid/18374
* SECUNIA:20639
* URL:http://secunia.com/advisories/20639

CVE Reference: CVE-2006-2379

New Vulnerabilities found this Week

KDE KDM Arbitrary File Reading Vulnerability
"Gain knowledge of sensitive information"

A vulnerability has been reported in KDE, which can be exploited by malicious, local users to gain knowledge of sensitive information.

KDM allows users to specify the session type for login, which is stored permanently in the user's home directory. This information is read insecurely by the "ReadDmrc()" function and can be exploited via symlink attacks to read the contents of any file on the system.

The vulnerability affects KDE 3.2.0 through 3.5.3.

References:
http://www.kde.org/info/security/advisory-20060614-1.txt

Sendmail Multi-Part MIME Message Handling Denial of Service
"Denial of Service"

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

The vulnerability is cause due to an error in the termination of the recursive "mime8to7()" function when performing MIME conversions. This can be exploited to cause a certain sendmail process to crash when it runs out of stack space while processing a deeply nested malformed MIME message.

Successful exploitation causes the delivery of other queued messages to fail or causes the generated core dump files to fill up available disk space.

The vulnerability has been reported in version 8.13.6 and prior.

References:
http://www.sendmail.org/releases/8.13.7.html
http://www.sendmail.com/security/advisories/SA-200605-01.txt.asc
http://www.kb.cert.org/vuls/id/146718

Symantec Security Information Manager Authentication Bypass
"obtain shell access"

A vulnerability has been reported in Symantec Security Information Manager, which can be exploited by malicious, local users to bypass certain security restrictions.

The vulnerability is caused due to an input validation error in the M4 Macro Library when transforming raw rule definitions into java code that can be executed by the rule-engine. This can be exploited via specially crafted rules to obtain shell access with privileges of the "sesuser" user during M4 transformation.

The vulnerability has been reported in version 4.0.2.

References:
http://securityresponse.symantec.com/avcenter/security/Content/2006.06.13b.html

Cisco WebVPN Cross-Site Scripting Vulnerability
"cross-site scripting attacks"

A vulnerability has been reported in Cisco WebVPN, which can be exploited by malicious people to conduct cross-site scripting attacks.

Input passed in the URL isn't properly sanitized before being returned to the user in the "dnserror.html" and the "connecterror.html" pages. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

Successful exploitation requires that clientless mode of the WebVPN feature is enabled.

The vulnerability has been reported in the following products:
* Cisco VPN 3000 Series Concentrators
* Cisco ASA 5500 Series Adaptive Security Appliances (ASA).

References:
http://lists.grok.org.uk/pipermail/full-disclosure/2006-June/046708.html
http://www.cisco.com/warp/public/707/cisco-sr-20060613-webvpn-xss.shtml

Microsoft Patch Tuesday

12 Microsoft Patches have been released this Tuesday.

References:
http://descriptions.securescout.com/tc/16264
http://descriptions.securescout.com/tc/16265

http://descriptions.securescout.com/tc/16266
http://descriptions.securescout.com/tc/16267
http://descriptions.securescout.com/tc/16268
http://descriptions.securescout.com/tc/16270
http://descriptions.securescout.com/tc/16271
http://descriptions.securescout.com/tc/16272
http://descriptions.securescout.com/tc/16273
http://descriptions.securescout.com/tc/16274
http://descriptions.securescout.com/tc/16275

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