netVigilance
assurance has arrived

2006 Issue # 41

ScoutNews

The weekly Security update from the makers of SecureScout

October 13, 2006

Table of Contents

Product Focus

Nimda Worm Scanner – The Nimda Worm 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 MS IE Mime Header Flaw (MS01-020) or have been infected by the Nimda Worm.

This Week in Review

Cyber identity theft flourishes. New technology enhances security on web services. Vista patchguard likely to be hacked. VoIP growing more secure.

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

- **Cybercrime flourishes in online hacker forums**

Criminals covet your identity data like never before. What's more, they've perfected more ways to access your bank accounts, grab your Social Security number and manipulate your identity than you can imagine.

Want proof? Just visit any of a dozen or so thriving cybercrime forums, Web sites that mirror the services of Amazon.com and the efficiencies of eBay. Criminal buyers and sellers convene at these virtual emporiums to wheel and deal in all things related to cyberattacks and in the fruit of cyberintrusions: pilfered credit and debit card numbers, hijacked bank accounts and stolen personal data.

The cybercrime forums gird a criminal economy that robs U.S. businesses of $67.2 billion a year, according to an FBI projection. Over the past two years, U.S. consumers lost more than $8 billion to viruses, spyware and online fraud schemes, Consumer Reports says.

Dailyrecord.com

Full Story :
http://dailyrecord.gns.gannettonline.com/apps/pbcs.dll/article?AID=/20061012/TECH01/609070348/1001/TECH

❖ Web services security enhanced by new technologies

With the new SecureSpan XML appliances Layer 7 Technologies announced at the Gartner Symposium/ ITxpo, that the the company is attempting to cover gamut of SOA, Web services and Web 2.0 technologies.
The suite of XML appliances and gateway software cover SOA, as well as what Layer 7 calls Web-Oriented Architectures (WOA), based on a variety of technologies including Ajax, SOAP, Plain Old XML (POX) and Representational State Transfer (REST), said Dimitri Sirota, the company's vice president for marketing and alliances.

"We are introducing whole family of XML security and networking solutions where for the first time, we're not only addressing SOA, but also Web 2.0," he said. "In addition to handling SOA, we're handling Web services more broadly, including Web 2.0. From our perspective, any application that's shared out to another application using any kind of XML protocol, SOAP, REST, POX, Ajax and so on, we can help secure, simplify and scale that infrastructure."

Computerweekly.com

Full Story :
http://www.computerweekly.com/Articles/2006/10/10/219153/Web+services+security+enhanced+by+new+technologies.htm

❖ Windows PatchGuard expected to be hacked soon

PatchGuard, a Microsoft technology to protect key parts of Windows, will be hacked sooner rather than later, a security expert said on Thursday.

Hackers will break through the protection mechanism soon after Microsoft releases Windows Vista, Aleksander Czarnowski, a technologist at Polish security company AVET Information and Network Security, said in a presentation at the Virus Bulletin event.

"It will probably take a year or so for it to surface publicly, but I believe it will be broken earlier," Czarnowski said. "PatchGuard will be broken pretty soon after the final version is released... A lot of people who would break it will probably not make it public immediately."

Zdnet uk

Full Story :
http://news.zdnet.co.uk/0,39020330,39284075,00.htm

- **VoIP tightens security against fuzzing, zombies, malicious intruders**

They may sound like fictitious Halloween characters, but for VoIP users, zombies and fuzzing are as real as they are scary.

Network intruders are leaping the fence from data networks over to the Voice over IP (VoIP) side, where they can easily take advantage of open source code for IP Telephony. There are similarities to the types of attacks already under way in the data world, but now they are being adapted to the VoIP world.

Is it time to start pulling our hair out and running for the hills?

Probably not. Security has already gained a lot of attention, and products are quickly becoming available that are dedicated specifically to VoIP. So while users should be proactive about preventing attacks, it's not yet time to panic, analysts, users and security vendors agree.

"What it has to come back to is the protocol.... A lot of the early VoIP systems were based on proprietary protocols that were vendor-specific. Vendors kept the details of those protocols to themselves," said Brendan Ziolo, director of marketing for Sipera, which makes the Sipera IPCS 310 system for comprehensive IP Communications Security. "Hackers didn't have the information they needed to launch an attack because the networks were very complicated then. They were closed in, and only legitimate traffic ran on the network."

Computerweekly.com

Full Story :
http://www.computerweekly.com/Articles/2006/10/05/219043/VoIP+tightens+security+against+fuzzing%2c+zombies%2c+malicious.htm

New Vulnerabilities Tested in SecureScout

- **16350 Vulnerability in ASP.NET 2.0 Could Allow Information Disclosure (MS06-056/922770) (Remote File Checking)**

A cross-site scripting vulnerability exists in a server running a vulnerable version of the .Net Framework 2.0 that could inject a client side script in the user's browser. The script could spoof content, disclose information, or take any action that the user could take on the affected web site. Attempts to exploit this vulnerability require user interaction.

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

References:

Original advisory:
* MS:MS06-056

http://www.microsoft.com/technet/security/Bulletin/MS06-056.mspx

Other references:
* US-CERT VU#455604:
http://www.kb.cert.org/vuls/id/455604

CVE Reference: CVE-2006-3436

❖ 16351 Vulnerability in Windows Explorer Could Allow Remote Execution (MS06-057/923191) (Remote File Checking)

A remote code execution vulnerability exists in Windows Shell due to improper validation of input parameters when invoked by the WebViewFolderIcon ActiveX control (Web View). This vulnerability could potentially allow remote code execution if a user visited a specially crafted Web site or viewed a specially crafted e-mail message. An attacker could exploit the vulnerability by hosting a web site that contained a web page that was used to exploit this vulnerability. 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:
* MS:MS06-057
http://www.microsoft.com/technet/security/Bulletin/MS06-057.mspx

Other references:
# BUGTRAQ:20060927 Exploit module available for WebViewFolderIcon setSlice 0-day
# URL:http://www.securityfocus.com/archive/1/archive/1/447174/100/0/threaded
# BUGTRAQ:20060930 ZERT patch for setSlice()
# URL:http://www.securityfocus.com/archive/1/archive/1/447490/100/0/threaded
# BUGTRAQ:20060930 setSlice exploited in the wild - massively
# URL:http://www.securityfocus.com/archive/1/archive/1/447426/100/0/threaded
# MISC: http://browserfun.blogspot.com/2006/07/mobb-18-webviewfoldericon-setslice.html
# MISC: http://riosec.com/msie-setslice-vuln
# MISC: http://isc.sans.org/diary.php?storyid=1742
# MISC: http://www.milw0rm.com/exploits/2440
# CERT:TA06-270A
# URL:http://www.us-cert.gov/cas/techalerts/TA06-270A.html
# CERT-VN:VU#753044
# URL:http://www.kb.cert.org/vuls/id/753044
# BID:19030
# URL:http://www.securityfocus.com/bid/19030
# OSVDB:27110
# URL:http://www.osvdb.org/27110
# SECTRACK:1016941
# URL:http://securitytracker.com/id?1016941
# SECUNIA:22159
# URL:http://secunia.com/advisories/22159
# XF:ie-webviewfoldericon-dos(27804)

URL:http://xforce.iss.net/xforce/xfdb/27804

CVE Reference: CVE-2006-3730

❖ 16352 Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (MS06-058/924163) (Remote File Checking)

A remote code execution vulnerability exists in PowerPoint. An attacker could exploit this vulnerability when PowerPoint parsed a file that included a malformed object pointer.

A remote code execution vulnerability exists in PowerPoint. An attacker could exploit this vulnerability when PowerPoint parsed a file that included a malformed Data record.

A remote code execution vulnerability exists in PowerPoint and could be exploited when PowerPoint opened a specially crafted file. Such a file might be included in an e-mail attachment or hosted on a malicious web site. An attacker could exploit the vulnerability by constructing a specially crafted PowerPoint file that could allow remote code execution.

A remote code execution vulnerability exists in PowerPoint and could be exploited when PowerPoint opened a specially crafted file. Such a file might be included in an e-mail attachment or hosted on a malicious web site. An attacker could exploit the vulnerability by constructing a specially crafted PowerPoint file that could allow remote code execution.

If a user were logged on with administrative user rights, an attacker who successfully exploited these vulnerabilities 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:
* MS:MS06-058
http://www.microsoft.com/technet/security/Bulletin/MS06-058.mspx

Other references:
* MISC: http://www.avertlabs.com/research/blog/?p=95
* MISC: http://vil.nai.com/vil/content/v_140666.htm
* MISC: http://www.microsoft.com/technet/security/advisory/925984.mspx
* URL:http://www.microsoft.com/technet/security/Bulletin/MS06-058.mspx
* CERT-VN:VU#231204
* URL:http://www.kb.cert.org/vuls/id/231204
* BID:20226
* URL:http://www.securityfocus.com/bid/20226
* FRSIRT:ADV-2006-3794
* URL:http://www.frsirt.com/english/advisories/2006/3794

* SECTRACK:1016937
* URL:http://securitytracker.com/id?1016937
* SECUNIA:22127
* URL:http://secunia.com/advisories/22127
* XF:powerpoint-presentation-file-code-execution(29225)
* URL:http://xforce.iss.net/xforce/xfdb/29225

CVE Reference: CVE-2006-3435

❖ 16353 Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (MS06-059/924164) (Remote File Checking)

A remote code execution vulnerability exists in Excel. An attacker could exploit this vulnerability when Excel parses a file and processes a malformed DATETIME record.

A remote code execution vulnerability exists in Excel. An attacker could exploit this vulnerability when Excel parses a file and processes a malformed STYLE record.

A remote code execution vulnerability exists in Excel. An attacker could exploit this vulnerability when Excel handles a Lotus 1-2-3 file.

A remote code execution vulnerability exists in Excel. An attacker could exploit this vulnerability when Excel parses a file and processes a malformed COLINFO record.

If a user were 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:
* MS:MS06-059
http://www.microsoft.com/technet/security/Bulletin/MS06-059.mspx

Other references:
* BUGTRAQ:20060703 Excel 2000/XP/2003 Style 0day POC
* URL:http://www.securityfocus.com/archive/1/archive/1/438963/100/0/threaded
* BUGTRAQ:20060707 Major updates to Excel 0-day Vulnerability FAQ at SecuriTeam Blogs
* URL:http://www.securityfocus.com/archive/1/archive/1/439427/100/0/threaded
* BUGTRAQ:20060711 New CVE number states Excel Style handling as a separate issue
* URL:http://marc.theaimsgroup.com/?l=bugtraq&m=115274676314243&w=2
* URL:http://www.microsoft.com/technet/security/Bulletin/MS06-059.mspx
* BID:18872
* URL:http://www.securityfocus.com/bid/18872
* FRSIRT:ADV-2006-2689
* URL:http://www.frsirt.com/english/advisories/2006/2689

* SECTRACK:1016430
* URL:http://securitytracker.com/id?1016430
* SECUNIA:20268
* URL:http://secunia.com/advisories/20268

CVE Reference: CVE-2006-2387

❖ 16354 Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (MS06-060/924554) (Remote File Checking)

A remote code execution vulnerability exists in Word. An attacker could exploit this vulnerability when Word parsed a file that contains a malformed string. Such a specially crafted file might be included as an e-mail attachment or hosted on a malicious web site. Viewing or previewing a malformed e-mail message in Outlook could not lead to exploitation of this vulnerability.

* Microsoft Word Mail Merge Vulnerability:

A remote code execution vulnerability exists in Microsoft Word, and could be exploited when Word opens a specially crafted mail merge file. Such a specially crafted file might be included as an e-mail attachment or hosted on a malicious web site. Viewing or previewing a malformed e-mail message in an affected version of Outlook could not lead to exploitation of this vulnerability. An attacker could exploit the vulnerability by constructing a specially crafted Word file that could allow remote code execution.

* Microsoft Word Malformed Stack Vulnerability:

A remote code execution vulnerability exists in Microsoft Word, and could be exploited when Word opens a specially crafted file. Such a specially crafted file might be included as an e-mail attachment or hosted on a malicious web site. Viewing or previewing a malformed e-mail message in an affected version of Outlook could not lead to exploitation of this vulnerability. An attacker could exploit the vulnerability by constructing a specially crafted Word file that could allow remote code execution.

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

References:

Original advisory:
* MS:MS06-060
http://www.microsoft.com/technet/security/Bulletin/MS06-060.mspx

Other references:
* BUGTRAQ:20060906 Microsoft confirmed Word 0-day vulnerability
* URL:http://www.securityfocus.com/archive/1/archive/1/445381/100/0/threaded
* BUGTRAQ:20060906 Re: Microsoft Word 0-day Vulnerability (September) FAQ document available
* URL:http://www.securityfocus.com/archive/1/archive/1/445285/100/0/threaded
* BUGTRAQ:20060905 Microsoft Word 0-day Vulnerability (September) FAQ document available
* URL:http://www.securityfocus.com/archive/1/archive/1/445162/100/100/threaded

* MISC: http://blogs.securiteam.com/?p=586
* MISC: http://isc.sans.org/diary.php?storyid=1669
* MISC:
http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2006-090219-2855-99
* MISC: http://vil.mcafeesecurity.com/vil/content/v_119055.htm
* CONFIRM: http://www.microsoft.com/technet/security/advisory/925059.mspx
* URL:http://www.microsoft.com/technet/security/Bulletin/MS06-060.mspx
* MSKB:Q925059
* URL:http://support.microsoft.com/kb/925059
* CERT-VN:VU#806548
* URL:http://www.kb.cert.org/vuls/id/806548
* BID:19835
* URL:http://www.securityfocus.com/bid/19835
* FRSIRT:ADV-2006-3448
* URL:http://www.frsirt.com/english/advisories/2006/3448
* OSVDB:28539
* URL:http://www.osvdb.org/28539
* SECTRACK:1016787
* URL:http://securitytracker.com/id?1016787
* SECUNIA:21735
* URL:http://secunia.com/advisories/21735
* XF:ms-word-code-execution(28775)
* URL:http://xforce.iss.net/xforce/xfdb/28775

CVE Reference:	CVE-2006-3647 CVE-2006-3651 CVE-2006-4534 CVE-2006-4693

❖ 16355 Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (MS06-061/924191) (Remote File Checking)

A vulnerability exists in Microsoft XML Core Services that could allow for information disclosure because the XMLHTTP ActiveX control incorrectly interprets an HTTP server-side redirect. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially lead to information disclosure if a user visited that page or clicked a link in a specially crafted e-mail message. An attacker who successfully exploited this vulnerability could access content from another domain retrieved using the credentials of the user browsing the Web at the client. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. However, user interaction is required to exploit this vulnerability.

A vulnerability exists in XSLT processing that could allow remote code execution on an affected system. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited that page. 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:
* MS:MS06-061
http://www.microsoft.com/technet/security/Bulletin/MS06-061.mspx

Other references:
US-CERT VU#703936:
http://www.kb.cert.org/vuls/id/703936

CVE Reference: CVE-2006-4685

❖ 16356 Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (MS06-062/922581) (Remote File Checking)

A remote code execution vulnerability exists in Office. An attacker could exploit this vulnerability when Office parses a file with a malformed string.

A remote code execution vulnerability exists in Office. An attacker could exploit this vulnerability when Office parses a file with a malformed chart record.

A remote code execution vulnerability exists in Office. An attacker could exploit this vulnerability when Office parses a file with a malformed record.

A remote code execution vulnerability exists in Microsoft Office, and could be exploited when Office opens a specially crafted file and parses a malformed Smart Tag. Such a specially crafted file might be included as an e-mail attachment or hosted on a malicious web site. Viewing or previewing a malformed e-mail message in Outlook could not lead to exploitation of this vulnerability. An attacker could exploit the vulnerability by constructing a specially crafted Office file that could allow remote code execution.

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

References:

Original advisory:
* MS:MS06-062
http://www.microsoft.com/technet/security/Bulletin/MS06-062.mspx

Other references:
* Fortinet:
http://www.fortinet.com/FortiGuardCenter/advisory/FG-2006-27.html
* Sowhat:
http://secway.org/advisory/AD20061010.txt
* ZDI:
http://www.zerodayinitiative.com/advisories/ZDI-06-034.html
* US-CERT VU#534276:
http://www.kb.cert.org/vuls/id/534276
* US-CERT VU#234900:
http://www.kb.cert.org/vuls/id/234900

* US-CERT VU#176556:
http://www.kb.cert.org/vuls/id/176556
* US-CERT VU#807780:
http://www.kb.cert.org/vuls/id/807780

CVE Reference: CVE-2006-3434

❖ 16357 Vulnerability in Server Service Could Allow Denial of Service and Remote Code Execution (MS06-063/923414) (Remote File Checking)

A denial of service vulnerability exists in the Server service because of the way it handles certain network messages. An attacker could exploit the vulnerability by sending a specially crafted network message to a computer running the Server service. An attacker who successfully exploited this vulnerability could cause the computer to stop responding.

A remote code execution vulnerability exists in the Server service because of the way it handles certain network messages. An attacker could exploit the vulnerability by sending a specially crafted network message to a system running the Server service as an authenticated user. While an attacker who successfully exploited this vulnerability could take complete control of the affected system, attempts to exploit this vulnerability will most probably result in a Denial of Service condition.

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

References:

Original advisory:
# MS:MS06-063
http://www.microsoft.com/technet/security/Bulletin/MS06-063.mspx

Other references:
# ISS:20060728 Vulnerability in Server Driver could result in Denial of Service
# URL:http://xforce.iss.net/xforce/alerts/id/231
# MISC: http://blogs.technet.com/msrc/archive/2006/07/28/443837.aspx
# MISC: http://www.milw0rm.com//exploits/2057
# BID:19215
# URL:http://www.securityfocus.com/bid/19215
# FRSIRT:ADV-2006-3037
# URL:http://www.frsirt.com/english/advisories/2006/3037
# OSVDB:27644
# URL:http://www.osvdb.org/27644
# SECTRACK:1016606
# URL:http://securitytracker.com/id?1016606
# SECUNIA:21276
# URL:http://secunia.com/advisories/21276
# XF:smb-malformed-pipe(27999)
# URL:http://xforce.iss.net/xforce/xfdb/27999

CVE Reference: CVE-2006-3942

❖ 16358 Vulnerabilities in TCP/IP IPv6 Could Allow Denial of Service (MS06-064/922819) (Remote File Checking)

A denial of service vulnerability exists in the IPv6 Windows implementation of the Internet Control Message Protocol (ICMP). An attacker who successfully exploited this vulnerability could cause the affected system to drop an existing TCP connection.

A denial of service vulnerability exists in the IPv6 Windows implementation of TCP. An attacker who successfully exploited this vulnerability could cause the affected system to drop an existing TCP connection.

A denial of service vulnerability exists in Windows in the IPv6 implementation of TCP/IP. An attacker who successfully exploited this vulnerability could cause the affected system to stop responding.

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

References:

Original advisory:
* MS:MS06-064
http://www.microsoft.com/technet/security/Bulletin/MS06-064.mspx

CVE Reference: CVE-2004-0790

❖ 16359 Vulnerability in Windows Object Packager Could Allow Remote Execution (MS06-065/924496) (Remote File Checking)

A remote code execution vulnerability exists in Windows Object Packager because of the way that file extensions are handled. An attacker could exploit the vulnerability by constructing a specially crafted file that could potentially allow remote code execution if a user visited a specially crafted Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, significant user interaction is required to exploit this vulnerability.

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

References:

Original advisory:
* MS06-065 (KB924496):
http://www.microsoft.com/technet/security/Bulletin/MS06-065.mspx

Other references:
* Secunia Research:
http://secunia.com/secunia_research/2006-54/
*US-CERT VU#703936:
http://www.kb.cert.org/vuls/id/703936

CVE Reference: CVE-2006-4692

New Vulnerabilities found this Week

Linksys SPA921 Long HTTP Requests Denial of Service
"Denial of Service"

Shawn Merdinger has reported a vulnerability in the Linksys SPA921 VoIP Phone, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to errors within the embedded HTTP server when handling long strings. This can be exploited to reboot the phone by sending long HTTP requests to it.

The vulnerability has been reported in firmware version 1.0.0. Other versions may also be affected.

References:
http://secunia.com/advisories/22267/

Linux Kernel "clip_mkip()" Denial of Service Vulnerability
"Denial of Service"

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

The vulnerability is caused due to an error in the "clip_mkip()" function in the ATM (Asynchronous Transfer Mode) subsystem and can be exploited to cause a kernel panic.

Successful exploitation requires installed ATM hardware and configured ATM support.

References:
http://www.redhat.com/support/errata/RHSA-2006-0689.html
http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=206265
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=fe26109a9dfd9327fdbe630fc819e1b7450986b2

Linksys WRT54GXv2 Insecure Universal Plug and Play Configuration
"Open arbitrary ports"

A vulnerability has been reported in Linksys WRT54GXv2, which can be exploited by malicious people to bypass certain security restrictions.

If Universal Plug and Play (UPnP) is enabled, the Linksys WRT54GXv2 also accepts UPnP requests sent to the WAN interface. This can e.g. be exploited to open arbitrary ports by sending an "AddPortMapping" command to the device.

The vulnerabilities have been reported in version 2.00.05. Other versions may also be affected.

References:
http://www.linksys.com/servlet/Satellite?c=L_Product_C2&childpagename=US%2FLayout&cid=1115416825933&pagename=Linksys%2FCommon%2FVisitorWrapper

Microsoft Windows Object Packager Dialog Spoofing Vulnerability

"Spoofing attacks"

Secunia Research has discovered a vulnerability in Microsoft Windows, which can be exploited by malicious people to conduct spoofing attacks.

The vulnerability is caused due to an input validation error in the Object Packager (packager.exe) in the handling of the "Command Line" property. This can be exploited to spoof the filename and the associated file type in the Packager security dialog by including a "/" slash character in the "Command Line" property.

This can further be exploited to execute arbitrary shell commands on a user's system by tricking a user into opening and interacting with e.g. a malicious Rich Text document or Word document containing an embedded Package object in e.g. WordPad.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-065.mspx
http://descriptions.securescout.com/tc/16359

Microsoft .NET Framework Cross-Site Scripting Vulnerability

"Cross-site scripting attacks"

A vulnerability has been reported in ASP.NET 2.0, which can be exploited by malicious people to conduct cross-site scripting attacks.

Certain input is not properly sanitised before being returned to the user. This can be exploited to execute arbitrary code in users browser-session associated with a vulnerable website.

Successful exploitation requires that the "AutoPostBack" feature is set to "true" (not the default setting).

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-056.mspx
http://descriptions.securescout.com/tc/16350

Microsoft XML Core Services Information Disclosure and Code Execution

"Disclose certain information"

Two vulnerabilities have been reported in Microsoft XML Core Services, which can be exploited by malicious people to disclose certain information and compromise a vulnerable system.

1) An unspecified error exists in the XMLHTTP ActiveX control when interpreting a HTTP server-side redirect. This can be exploited to disclose certain information e.g. via a specially crafted web page.

2) A boundary error exists in the XSLT processing in MSXML. This can be exploited to cause a buffer overflow via a specially crafted web page and allows execution of arbitrary code.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-061.mspx
http://descriptions.securescout.com/tc/16355

Microsoft Office Multiple Code Execution Vulnerabilities

"Buffer overflow"

Multiple vulnerabilities have been reported in Microsoft Office, which can be exploited by malicious people to compromise a user's system.

1) An unspecified boundary error within the parsing of certain strings can be exploited to cause a buffer overflow via a specially crafted Office document.

2) A boundary error when parsing chart records can be exploited to cause a buffer overflow via a specially crafted Office document.

3) An unspecified boundary error in mso.dll when parsing certain records can be exploited to cause a buffer overflow via a specially crafted Office document.

4) A boundary error within the parsing of Smart Tags can be exploited to cause a buffer overflow via a specially crafted Office document.

Successful exploitation of the vulnerabilities allows execution of arbitrary code.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-062.mspx
http://descriptions.securescout.com/tc/16356
http://descriptions.securescout.com/tc/16352
http://descriptions.securescout.com/tc/16353
http://descriptions.securescout.com/tc/16354

Microsoft Windows Multiple IPv6 Denial of Service Vulnerabilities

"Denial of Service"

Three vulnerabilities have been reported in Microsoft Windows, which can be exploited by malicious people to cause a DoS (Denial of Service).

1) A vulnerability exists in the IPv6 Windows implementation of ICMP which, if successfully exploited, results in the system dropping an existing connection.

2) A vulnerability exists in the IPv6 Windows implementation of TCP which, if successfully exploited, results in the system dropping an existing TCP connection.

3) A vulnerability exists in the IPv6 implementation of TCP/IP which, if successfully exploited, could cause the system to stop responding.

Successful exploitation of the vulnerabilities requires IPv6 to be configured (not enabled by default).

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-064.mspx
http://descriptions.securescout.com/tc/16358

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