netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 15 April 14, 2006

Table of Contents

Product Focus

This Week in Review

White hats resort to Vigilante justice, Black hats continue to develop more sophisticated DDoS attack methods and Microsoft bungles patch Tuesday bundles.

Enjoy reading

Call or email netVigilance to get an update on SecureScout.
(503) 524 5758 or sales@netVigilance.com

Top Security News Stories this Week

- **White Hat volunteers dedicated to shutting down Phishers**

A group of volunteer ethical hackers calling themselves the Phishing Incident Reporting and Termination squad (PIRT), have taken to hunting down phishers and shutting them down. This Vigilante[1] organization reports phishing scams to law enforcement and security organizations and takes actions to terminate phishing sites. This group White Hat hackers are formed from employees of CastleCops, a security

[1] (Hey, not a bad name for a security company – *Ed.*)

and privacy organization, and Sunbelt Software.
RedHerring

Full Story :
http://www.redherring.com/Article.aspx?a=16352&hed=Vigilantes+Go+After+Phishers&sector=Industries&subsector=SecurityAndDefense

- **Another disturbing trend in DDoS Attacks**

Richard Stiennon reports on a new type of Zombie that is being deployed by hackers to launch Distributed Denial of Service (DDoS)attacks on web servers. Typically Zombies or bot-net herds are collections of PCs on college campuses or in homes that are hacked and used to launch hacker attacks by proxy.

In this recently discovered DDoS attack style, the hackers are utilizing web servers on broadband connections; giving them access to much higher bandwidth connections and further anonymity. Another recent new technique involves using zombies to simultaneously perform DNS look-ups; overwhelming the DNS server for the target. This method of attack causes the DNS server to die, taking down a site without even hitting it directly.
ZDNet

Full Story:
http://blogs.zdnet.com/threatchaos/index.php?p=310

- **Microsoft raises ire by bundling IE changes with patches.**

Many security professionals are up in arms in response to Microsoft's decision to include functionality change for Internet Explorer with a needed security update. By seriously impacting the ability to deply and test necessary patches; experts are questioning why the OS giant did not release these changes in a separate update of Service Pack.
TechWeb News

Full Story:
http://se.securitypipeline.com/showArticle.jhtml?articleID=185300871

New Vulnerabilities Tested in SecureScout

- **16200 Cumulative Security Update for Internet Explorer (MS06-**

013/912812) (Remote File Checking)

A remote code execution vulnerability exists in the way Internet Explorer displays a Web page that contains certain unexpected method calls to HTML objects. As a result, system memory may be corrupted in such a way that an attacker could execute arbitrary code if a user visited a malicious Web site.

A remote code execution vulnerability exists in the way Internet Explorer handles multiple event handlers in an HTML element. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited the malicious Web site.

A remote code execution vulnerability exists in Internet Explorer. An HTML Application (HTA) can be initiated in a way that bypasses the security control within Internet Explorer. This allows an HTA to execute without Internet Explorer displaying the normal security dialog box. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited the malicious Web site.

A remote code execution vulnerability exists in the way Internet Explorer handles specially crafted and not valid HTML. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited the malicious Web site.

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 malicious Web page that could potentially allow remote code execution if a user visited the malicious Web site.

A remote code execution vulnerability exists in the way Internet Explorer handles HTML elements that contain a specially crafted tag. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited the malicious Web site.

A remote code execution vulnerability exists in the way Internet Explorer handles double-byte characters in specially crafted URLs. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited the malicious Web site.

An attacker who successfully exploited any of these vulnerabilities could take complete control of an affected system.

A vulnerability exists in Internet Explorer in the way it returns IOleClientSite information when an embedded object is dynamically created. An attacker could exploit the vulnerability by constructing a malicious Web page with a dynamically created object. This object would need to make use of the IOleClientSite information returned to make a security related decision. This could potentially allow remote code execution or information disclosure if a user visited the malicious Web site.

An information disclosure vulnerability exists in Internet Explorer because of the way that it handles navigation methods. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially lead to information disclosure if a user visited a malicious Web site or viewed a specially crafted e-mail message. An attacker who successfully exploited this vulnerability could read cookies or other 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 has been navigated away from the attacker's Web site but the content of the window still contains the attacker's Web page.

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

References:

Original advisory:
MS:MS06-013
http://www.microsoft.com/technet/security/bulletin/ms06-013.mspx

Other references:
* BUGTRAQ:20060322 IE crash
* URL:http://www.securityfocus.com/archive/1/428441
* BUGTRAQ:20060322 Microsoft Internet Explorer (mshtml.dll) - Remote Code Execution
* URL:http://www.securityfocus.com/archive/1/archive/1/428583/100/0/threaded
* BUGTRAQ:20060328 EEYE: Temporary workaround for IE createTextRange vulnerability
* URL:http://www.securityfocus.com/archive/1/archive/1/429088/100/0/threaded
* MISC:http://www.computerterrorism.com/research/ct22-03-2006
* BUGTRAQ:20060323 Secunia Research: Microsoft Internet Explorer "createTextRange()"Code Execution
* URL:http://www.securityfocus.com/archive/1/archive/1/428600/100/0/threaded
* MISC:http://secunia.com/secunia_research/2006-7/advisory/
* CONFIRM:http://www.microsoft.com/technet/security/advisory/917077.mspx
* CERT:TA06-101A
* URL:http://www.us-cert.gov/cas/techalerts/TA06-101A.html
* CERT-VN:VU#876678
* URL:http://www.kb.cert.org/vuls/id/876678
* BID:17196
* URL:http://www.securityfocus.com/bid/17196
* FRSIRT:ADV-2006-1050
* URL:http://www.frsirt.com/english/advisories/2006/1050
* FRSIRT:ADV-2006-1318
* URL:http://www.frsirt.com/english/advisories/2006/1318
* OSVDB:24050
* URL:http://www.osvdb.org/24050
* SECTRACK:1015812
* URL:http://securitytracker.com/id?1015812
* SECUNIA:18680
* URL:http://secunia.com/advisories/18680
* XF:ie-createtextrange-command-execution(25379)
* URL:http://xforce.iss.net/xforce/xfdb/25379
* BUGTRAQ:20060316 Remote overflow in MSIE script action handlers (mshtml.dll)
* URL:http://archives.neohapsis.com/archives/bugtraq/2006-02/0855.html
* BUGTRAQ:20060325 Re: [optimized PoC] Remote overflow in MSIE script action handlers (mshtml.dll)
* URL:http://www.securityfocus.com/archive/1/archive/1/428810/100/0/threaded
* CERT-VN:VU#984473
* URL:http://www.kb.cert.org/vuls/id/984473
* BID:17131
* URL:http://www.securityfocus.com/bid/17131

* OSVDB:23964
* URL:http://www.osvdb.org/23964
* SECTRACK:1015794
* URL:http://securitytracker.com/id?1015794
* SECUNIA:19269
* URL:http://secunia.com/advisories/19269
* SECUNIA:18957
* URL:http://secunia.com/advisories/18957
* XF:ie-mshtml-bo(25292)
* URL:http://xforce.iss.net/xforce/xfdb/25292
* MISC:http://jeffrey.vanderstad.net/grasshopper/
* MISC:http://news.zdnet.com/2100-1009_22-6052396.html?tag=zdfd.newsfeed
* CERT-VN:VU#434641
* URL:http://www.kb.cert.org/vuls/id/434641
* BID:17181
* URL:http://www.securityfocus.com/bid/17181
* OSVDB:24095
* URL:http://www.osvdb.org/24095
* SECTRACK:1015800
* URL:http://securitytracker.com/id?1015800
* SECUNIA:19378
* URL:http://secunia.com/advisories/19378
* XF:ie-hta-file-execution(25394)
* URL:http://xforce.iss.net/xforce/xfdb/25394
* CERT-VN:VU#503124
* URL:http://www.kb.cert.org/vuls/id/503124
* URL:http://secunia.com/advisories/18957
* BID:17453
* URL:http://www.securityfocus.com/bid/17453
* CERT-VN:VU#824324
* URL:http://www.kb.cert.org/vuls/id/824324
* CERT-VN:VU#341028
* URL:http://www.kb.cert.org/vuls/id/341028
* CERT-VN:VU#959649
* URL:http://www.kb.cert.org/vuls/id/959649
* BID:17455
* URL:http://www.securityfocus.com/bid/17455
* BID:17460
* URL:http://www.securityfocus.com/bid/17460

CVE Reference: CVE-2006-1359, CVE-2006-1245, CVE-2006-1388, CVE-2006-1185, CVE-2006-1186, CVE-2006-1188, CVE-2006-1189, CVE-2006-1190, CVE-2006-1191, CVE-2006-1192

❖ 16201 Vulnerability in the Microsoft Data Access Components (MDAC) Function Could Allow Code Execution (MS06-014/911562) (Remote File Checking)

A remote code execution vulnerability exists in the RDS.Dataspace ActiveX control that is provided as part of the ActiveX Data Objects (ADO) and that is distributed in MDAC. An attacker who successfully exploited this vulnerability could take complete control of an affected system

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

References:

Original advisory:
* MS:MS06-014
* URL:http://www.microsoft.com/technet/security/bulletin/ms06-014.mspx

Other references:
* CERT:TA06-101A
* URL:http://www.us-cert.gov/cas/techalerts/TA06-101A.html
* CERT-VN:VU#234812
* URL:http://www.kb.cert.org/vuls/id/234812
* BID:17462
* URL:http://www.securityfocus.com/bid/17462
* FRSIRT:ADV-2006-1319
* URL:http://www.frsirt.com/english/advisories/2006/1319
* SECUNIA:19583
* URL:http://secunia.com/advisories/19583

CVE Reference: CVE-2006-000

❖ 16202 Vulnerability in Windows Explorer Could Allow Remote Code Execution (MS06-015/908531) (Remote File Checking)

A remote code execution vulnerability exists in Windows Explorer because of the way that it handles COM objects. An attacker would need to convince a user to visit a Web site that could force a connection to a remote file server. This remote file server could then cause Windows Explorer to fail in a way that could allow code execution. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

References:

Original advisory:
* MS:MS06-015
* URL:http://www.microsoft.com/technet/security/bulletin/ms06-015.mspx

Other references:
* CERT:TA06-101A
* URL:http://www.us-cert.gov/cas/techalerts/TA06-101A.html
* BID:17464
* URL:http://www.securityfocus.com/bid/17464
* FRSIRT:ADV-2006-1320
* URL:http://www.frsirt.com/english/advisories/2006/1320
* SECUNIA:19606
* URL:http://secunia.com/advisories/19606
* CERT-VN:VU#641460
* URL:http://www.kb.cert.org/vuls/id/641460

CVE Reference: CVE-2006-001

❖ 16203 Cumulative Security Update for Outlook Express (MS06-016/911567) (Remote File Checking)

A remote code execution vulnerability exists in Outlook Express when using a Windows Address Book (.wab) file that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

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: **High** Risk: **Attack**

References:

Original advisory:
* MS:MS06-016
* URL:http://www.microsoft.com/technet/security/bulletin/ms06-016.mspx

Other references:
* BUGTRAQ:20060411 ZDI-06-007: Microsoft Windows Address Book (WAB) File Format Parsing Vulnerability
* URL:http://www.securityfocus.com/archive/1/archive/1/430645/100/0/threaded
* MISC:http://www.zerodayinitiative.com/advisories/ZDI-06-007.html
* BID:17459
* URL:http://www.securityfocus.com/bid/17459
* FRSIRT:ADV-2006-1321
* URL:http://www.frsirt.com/english/advisories/2006/1321
* SECUNIA:19617
* URL:http://secunia.com/advisories/19617

CVE Reference: CVE-2006-0014

❖ 16204 Vulnerability in Microsoft FrontPage Server Extensions Could Allow Cross-Site Scripting (MS06-017/917627) (Remote File Checking)

The cross-site scripting vulnerability could allow an attacker to run client-side script on behalf of an FPSE user. 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. An attacker who successfully exploited this vulnerability against an administrator could take complete control of a Front Page Server Extensions 2002 server.

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

References:

Original advisory:
* MS:MS06-017
* URL:http://www.microsoft.com/technet/security/Bulletin/MS06-017.mspx

Other references:
* FRSIRT:ADV-2006-1322
* URL:http://www.frsirt.com/english/advisories/2006/1322
* SECUNIA:19623
* URL:http://secunia.com/advisories/19623

CVE Reference: CVE-2006-0015

❖ 16205 Linux Kernel SYSFS Local Denial of Service Vulnerability

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

The vulnerability is caused due to an out-of-bounds memory error in the "fill_write_buffer()" function in sysfs/file.c when writing exactly PAGE_SIZE amount of data with no zeroes in it to a sysfs file.

The vulnerability has been reported in versions 2.6 through 2.6.16.1.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.2

Other references:
* CONFIRM:http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=6e0dd741a89be35defa05bd79f4211c5a2762825
* CONFIRM:http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=6e0dd741a89be35defa05bd79f4211c5a2762825;hp=597a7679dd83691be2f3a53e1f3f915b4a7f6eba
* TRUSTIX:2006-0020
* URL:http://www.trustix.org/errata/2006/0020
* BID:17402
* URL:http://www.securityfocus.com/bid/17402
* FRSIRT:ADV-2006-1273
* URL:http://www.frsirt.com/english/advisories/2006/1273
* SECUNIA:19495
* URL:http://secunia.com/advisories/19495

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-1055

❖ 16206 Linux Kernel "__keyring_search_one()" Denial of Service

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

The vulnerability is caused due to an error in the "__keyring_search_one()" function when adding a key to a non-keyring key.

The vulnerability has been reported in versions 2.6 through 2.6.16.2.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.3

Other references:
* CONFIRM:https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=188466
* CONFIRM:http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=c3a9d6541f84ac3ff566982d08389b87c1c36b4e
* BID:17451
* URL:http://www.securityfocus.com/bid/17451
* SECUNIA:19573
* URL:http://secunia.com/advisories/19573

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-1522

❖ 16207 PHP "phpinfo()" arbitrary HTML and script code execution Vulnerability

Maksymilian Arciemowicz has reported a vulnerability in PHP, which can be exploited by malicious, local users to conduct cross-site scripting attacks and execute arbitrary HTML and script code.

The "phpinfo()" PHP function only sanitises the first 4096 characters of an array request parameter before it is returned to users. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site via a script calling "phpinfo()".

The issue has been fixed in PHP versions 4.4.3 and 5.1.3.

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

References:

Original Advisory:
http://securityreason.com/achievement_securityalert/34

Other references:
* BUGTRAQ:20060409 phpinfo() Cross Site Scripting PHP 5.1.2 and 4.4.2
* URL:http://www.securityfocus.com/archive/1/archive/1/430449/100/0/threaded

* FULLDISC:20060408 phpinfo() Cross Site Scripting PHP 5.1.2 and 4.4.2
* URL:http://lists.grok.org.uk/pipermail/full-disclosure/2006-April/044981.html
* MISC:http://securityreason.com/achievement_securityalert/34
* MLIST:[php-cvs] 20060330 cvs: php-src /ext/standard info.c
* URL:http://marc.theaimsgroup.com/?l=php-cvs&m=114374620416389&w=2
* CONFIRM:http://cvs.php.net/viewcvs.cgi/php-src/ext/standard/info.c
* CONFIRM:http://cvs.php.net/viewcvs.cgi/php-src/ext/standard/info.c?r1=1.260&r2=1.261
* BID:17362
* URL:http://www.securityfocus.com/bid/17362
* FRSIRT:ADV-2006-1290
* URL:http://www.frsirt.com/english/advisories/2006/1290
* SECTRACK:1015879
* URL:http://securitytracker.com/id?1015879
* SECUNIA:19599
* URL:http://secunia.com/advisories/19599

Product Page:
http://www.php.net/

CVE Reference: CVE-2006-099

❖ 16208 PHP error in "tempnam()" to be exploited to bypass security restrictions

Maksymilian Arciemowicz has reported a vulnerability in PHP, which can be exploited by malicious, local or remote users to bypass security restrictions.

An error in the "tempnam()" PHP function can be exploited to bypass the "open_basedir" directive and create temporary files in arbitrary directories via directory traversal attacks.

The issue has been fixed in PHP versions 4.4.3 and 5.1.3.

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

References:

Original Advisory:
http://securityreason.com/achievement_securityalert/36

Other references:
* BUGTRAQ:20060409 tempnam() open_basedir bypass PHP 4.4.2 and 5.1.2
* URL:http://www.securityfocus.com/archive/1/archive/1/430456/100/0/threaded
* MISC:http://securityreason.com/achievement_securityalert/36
* FRSIRT:ADV-2006-1290
* URL:http://www.frsirt.com/english/advisories/2006/1290
* SECTRACK:1015881
* URL:http://securitytracker.com/id?1015881
* SECUNIA:19599
* URL:http://secunia.com/advisories/19599

Product Page:

http://www.php.net/

CVE Reference: CVE-2006-1494

❖ 16209 PHP error in the "copy()" to be exploited to bypass the safe mode protection mechanism

Maksymilian Arciemowicz has reported a vulnerability in PHP, which can be exploited by malicious, local users to bypass the safe mode protection mechanism.

An error in the "copy()" PHP function can be exploited to bypass the safe mode protection mechanism and access files outside the "open_basedir" root via the "compress.zlib://" file wrapper.

The issue has been fixed in PHP versions 4.4.3 and 5.1.3.

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

References:

Original Advisory:
http://securityreason.com/achievement_securityalert/37

Other references:
* BUGTRAQ:20060409 copy() Safe Mode Bypass PHP 4.4.2 and 5.1.2
* URL:http://www.securityfocus.com/archive/1/archive/1/430461/100/0/threaded
* MISC:http://securityreason.com/achievement_securityalert/37
* FRSIRT:ADV-2006-1290
* URL:http://www.frsirt.com/english/advisories/2006/1290
* SECTRACK:1015882
* URL:http://securitytracker.com/id?1015882
* SECUNIA:19599
* URL:http://secunia.com/advisories/19599

Product Page:
http://www.php.net/

CVE Reference: CVE-2006-1608

New Vulnerabilities found this Week

Sun Solaris LDAP2 Client Commands Security Issue
"Gain knowledge of sensitive information"

A security issue has been reported in Sun Solaris, which can be exploited by malicious, local users to gain knowledge of sensitive information.

The problem is that the Directory Server rootDN (Distinguished Name) password may be disclosed to local users when a privileged users runs the idsconfig command or certain LDAP commands (ldapadd, ldapdelete, ldapmodify, ldapmodrdn, and ldapsearch).

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102113-1

Sun Solaris "sh" Process Denial of Service Vulnerability
"Denial of Service"

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

The vulnerability is caused due to an unspecified error in the Bourne shell when creating temporary files and can be exploited to crash "sh" processes on a system.
References:

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102282-1

Cyrus SASL DIGEST-MD5 Pre-Authentication Denial of Service
"Denial of Service"

Mu Security has reported a vulnerability in Cyrus SASL library, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an unspecified error during DIGEST-MD5 negotiation.

The vulnerability has been reported in version 2.1.18. Other versions may also be affected.
References:

References:
http://labs.musecurity.com/advisories/MU-200604-01.txt

Microsoft FrontPage Server Extensions Cross-Site Scripting
"Cross-site scripting attacks"

Esteban Martínez Fayó has reported a vulnerability in Microsoft FrontPage Server Extensions, which can be exploited by malicious people to conduct cross-site scripting attacks.

Input passed to the "operation", "command", and "name" parameters in "/_vti_bin/_vti_adm/fpadmdll.dll", which is used for administrative purposes, is not properly sanitised before being returned to users. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-017.mspx
http://www.argeniss.com/research/ARGENISS-ADV-040602.txt
http://descriptions.securescout.com/tc/16204

Microsoft Data Access Components RDS.Dataspace ActiveX Vulnerability

“Compromise a vulnerable system”

A vulnerability has been reported in Microsoft Data Access Components (MDAC), which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an unspecified error in the behavior of the RDS.Dataspace ActiveX control as it fails to ensure that it interacts safely with a web site.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-014.mspx
http://descriptions.securescout.com/tc/16201

Internet Explorer Multiple Vulnerabilities
“Cross-site scripting attacks, conduct phishing attacks”

Multiple vulnerabilities have been reported in Internet Explorer, which can be exploited by malicious people to conduct cross-site scripting attacks, conduct phishing attacks, or compromise a user's system.

1) An error in the cross-domain restriction when accessing properties of certain dynamically created objects can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an arbitrary site via a JavaScript URI handler applied on a dynamically created "object" tag.

2) An error within the handling of multiple event handlers (e.g. onLoad) in an HTML element can be exploited to corrupt memory in a way that may allow execution of arbitrary code.

3) An error within the parsing of specially crafted, non-valid HTML can be exploited to corrupt memory in a way that allows execution of arbitrary code when a malicious HTML document is viewed.

4) An error within the instantiation of COM objects that are not intended to be instantiated in Internet Explorer can be exploited to corrupt memory in a way that allows execution of arbitrary code.

5) An error within the handling of HTML elements containing a specially crafted tag can be exploited to corrupt memory in a way that allows execution of arbitrary code.

6) An error within the handling of double-byte characters in specially crafted URLs can be exploited to corrupt memory in a way that allows execution of arbitrary code.

Successful exploitation requires that the system uses double-byte character sets.

7) An error in the way IOleClientSite information is returned when an embedded object is dynamically created can be exploited to execute arbitrary code in context of another site or security zone.

8) An unspecified error can be exploited to spoof information displayed in the address bar and other parts of the trust UI.

9) Some unspecified vulnerabilities exist in the two ActiveX controls included with Danim.dll and Dxtmsft.dll.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-013.mspx
http://descriptions.securescout.com/tc/16200

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