netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 20

May 16, 2008

Table of Contents

Product Focus

Much anticipated "Negev" released.

Our Web-interface for the Perimeter Service is now running dynamic pages based on "Ajax", giving a much improved response time and customer experience. Existing customers can log right into the new system from the usual login page.

Spida Digispid Worm Scanner – The Spida Digispid Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are prone any of the Microsoft Java Virtual Machine Vulnerabilities (MS02-069).

CTO Jesper Jurcenoks of netVigilance is the keynote speaker at the ITEC Conference & Exhibition 2008 in Dallas June 4-5, see
http://www.netvigilance.com/events

This Week in Review

Update to PCI Security standards expected. SQL injections getting very sophisticated. Suggestion from the military to use the hacker's very own weapon. Another look at VoIP security.

Enjoy reading & Stay safe.

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

Top Security News Stories this Week

❖ PCI standard version 1.2 expected out in October

The second installment of the Payment Card Industry Data Security Standard (PCI DSS) is due out in the fall.

PCI DSS version 1.2, the first update since September 2006 when the PCI Security Standards Council began driving the standard, is due out in October and incorporated feedback from some 450 participating organization, the council announced Wednesday.

The council said it tapped into recommendations from retailers, security product vendors, electronic funds transfer networks, point-of-sale application developers and banks.

scmagazine

Full Story :
http://www.scmagazineus.com/PCI-standard-version-12-expected-out-in-October/article/110165/

❖ SQL injection attack in 'third wave,' says IBM

A SQL injection attack that has affected at least a half-million Web sites has entered a "third wave" that's more resistant than previous versions to traditional security measures, according to IBM security researchers.
"I've been tracking SQL injections for the last five or six years. This is some of the most intricate obfuscation I've ever seen," says David Dewey, research manager for the X-Force technology at IBM's Internet Security Systems division. (Compare security products.)

A SQL injection is an attack against a database-driven Web site in which the hacker executes unauthorized SQL commands by taking advantage of insecure code on systems connected to the Internet.

networkworld

Full Story :
http://www.networkworld.com/news/2008/051508-sql-injection-attack-third-wave.html?fsrc=netflash-rss

❖ A U.S. Military Botnet?

A U.S. Air Force colonel has proposed the creation of a military botnet to unleash against the hackers, especially the computer networks of foreign powers.

Botnets have become one of the hazards of modern life. They spew out spam by the truckload, and can be utilized for denial of service attacks. Now U.S. Air Force colonel Charles Williamson III has come up with a novel idea, according to AP. In the May ediдtion of Armed Forces Journal the Colonel has proposed the formation of a military

botnet that could be used against hackers and foreign powers to assert dominance – or at least defense – in cyberspace.

Digital trends

Full Story :
http://news.digitaltrends.com/news-article/16718/a-u-s-military-botnet

- **VoIP Security: SIP—Versatile but Vulnerable**

As a mission critical service, VoIP deployments require careful assessment to identify and eliminate security vulnerabilities in VoIP clients, applications, and infrastructure. But what exactly should you hunt for? Let's explore a few security cracks commonly found in VoIP products that use SIP.
Something old, something new
Many VoIP handsets and softphones use SIP signaling to register with a server and place or receive calls through a proxy. During calls, voice is digitized, encoded, compressed, and transported by RTP messages between calling and called parties (SIP user agents). Those SIP and RTP messages are exchanged over IP networks—hence the moniker Voice over IP.

VoIPPlanet

Full Story :
http://www.voipplanet.com/solutions/article.php/3747161

New Vulnerabilities Tested in SecureScout

- **13634 MySQL RENAME TABLE overwrite system table information and gain privileges Vulnerability**

MySQL Community Server 5.0.x before 5.0.51, Enterprise Server 5.0.x before 5.0.52, Server 5.1.x before 5.1.23, and Server 6.0.x before 6.0.4, when a table relies on symlinks created through explicit DATA DIRECTORY and INDEX DIRECTORY options, allows remote authenticated users to overwrite system table information and gain privileges via a RENAME TABLE statement that changes the symlink to point to an existing file.

The security issue has been reported in versions:
MySQL Community Server 5.0.x before 5.0.51, Enterprise Server 5.0.x before 5.0.52, Server 5.1.x before 5.1.23, and Server 6.0.x before 6.0.4.

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

References:

CVE Reference:

CVE-2007-5969 (cve.mitre.org, nvd.nist.gov)

- **13635 MySQL CREATE SQL SECURITY DEFINER VIEW, and ALTER VIEW statements gain privileges Vulnerability**

MySQL 5.0.x before 5.0.51a, 5.1.x before 5.1.23, and 6.0.x before 6.0.4 does not update the DEFINER value of a view when the view is altered, which allows remote authenticated users to gain privileges via a sequence of statements including a CREATE SQL SECURITY DEFINER VIEW statement and an ALTER VIEW statement.

The security issue has been reported in versions:
MySQL 5.0.x before 5.0.52, 5.1.x before 5.1.23, and 6.0.x before 6.0.4

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

References:

* BUGTRAQ: 20080205 rPSA-2008-0040-1 mysql mysql-bench mysql-server
http://www.securityfocus.com/archive/1/archive/1/487606/100/0/threaded
* CONFIRM:
http://bugs.mysql.com/bug.php?id=29908
* CONFIRM:
http://dev.mysql.com/doc/refman/5.0/en/releasenotes-es-5-0-52.html
* CONFIRM:
http://dev.mysql.com/doc/refman/5.1/en/news-5-1-23.html
* CONFIRM:
http://dev.mysql.com/doc/refman/6.0/en/news-6-0-4.html
* CONFIRM:
http://lists.mysql.com/announce/502
* CONFIRM:
https://issues.rpath.com/browse/RPL-2187
* CONFIRM:
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0040
* FEDORA: FEDORA-2007-4465
https://www.redhat.com/archives/fedora-package-announce/2007-December/msg00467.html
* FEDORA: FEDORA-2007-4471
https://www.redhat.com/archives/fedora-package-announce/2007-December/msg00475.html
* GENTOO: GLSA-200804-04
http://security.gentoo.org/glsa/glsa-200804-04.xml
* MANDRIVA: MDVSA-2008:017
http://www.mandriva.com/security/advisories?name=MDVSA-2008:017
* REDHAT: RHSA-2007:1157
http://www.redhat.com/support/errata/RHSA-2007-1157.html
* SUSE: SUSE-SR:2008:003
http://lists.opensuse.org/opensuse-security-announce/2008-02/msg00003.html
* UBUNTU: USN-588-1
http://www.ubuntu.com/usn/usn-588-1
* BID: 26832
http://www.securityfocus.com/bid/26832
* FRSIRT: ADV-2007-4198
http://www.frsirt.com/english/advisories/2007/4198
* SECTRACK: 1019085
http://securitytracker.com/id?1019085
* SECUNIA: 28063

http://secunia.com/advisories/28063
* SECUNIA: 28025
http://secunia.com/advisories/28025
* SECUNIA: 28739
http://secunia.com/advisories/28739
* SECUNIA: 28838
http://secunia.com/advisories/28838
* SECUNIA: 29443
http://secunia.com/advisories/29443
* SECUNIA: 29706
http://secunia.com/advisories/29706
* XF: mysql-definer-value-privilege-escalation(38989)
http://xforce.iss.net/xforce/xfdb/38989

CVE Reference:

CVE-2007-6303 (cve.mitre.org, nvd.nist.gov)

- **13636 MySQL federated engine, SHOW TABLE STATUS query Denial of Service Vulnerability**

The federated engine in MySQL 5.0.x before 5.0.51a, 5.1.x before 5.1.23, and 6.0.x before 6.0.4, when performing a certain SHOW TABLE STATUS query, allows remote MySQL servers to cause a denial of service (federated handler crash and daemon crash) via a response that lacks the minimum required number of columns.

The security issue has been reported in versions:
MySQL 5.0.x before 5.0.52, 5.1.x before 5.1.23, and 6.0.x before 6.0.4

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

References:

* BUGTRAQ: 20080205 rPSA-2008-0040-1 mysql mysql-bench mysql-server
http://www.securityfocus.com/archive/1/archive/1/487606/100/0/threaded
* CONFIRM:
http://bugs.mysql.com/bug.php?id=29801
* CONFIRM:
http://dev.mysql.com/doc/refman/5.0/en/releasenotes-es-5-0-52.html
* CONFIRM:
http://dev.mysql.com/doc/refman/5.1/en/news-5-1-23.html
* CONFIRM:
http://dev.mysql.com/doc/refman/6.0/en/news-6-0-4.html
* CONFIRM:
http://lists.mysql.com/announce/502
* CONFIRM:
https://issues.rpath.com/browse/RPL-2187
* CONFIRM:
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0040
* DEBIAN: DSA-1451
http://www.debian.org/security/2008/dsa-1451
* GENTOO: GLSA-200804-04
http://security.gentoo.org/glsa/glsa-200804-04.xml

* MANDRIVA: MDVSA-2008:017
http://www.mandriva.com/security/advisories?name=MDVSA-2008:017
* MANDRIVA: MDVSA-2008:028
http://www.mandriva.com/security/advisories?name=MDVSA-2008:028
* SUSE: SUSE-SR:2008:003
http://lists.opensuse.org/opensuse-security-announce/2008-02/msg00003.html
* UBUNTU: USN-559-1
http://www.ubuntulinux.org/support/documentation/usn/usn-559-1
* BID: 26832
http://www.securityfocus.com/bid/26832
* FRSIRT: ADV-2007-4198
http://www.frsirt.com/english/advisories/2007/4198
* SECTRACK: 1019085
http://securitytracker.com/id?1019085
* SECUNIA: 28063
http://secunia.com/advisories/28063
* SECUNIA: 28128
http://secunia.com/advisories/28128
* SECUNIA: 28343
http://secunia.com/advisories/28343
* SECUNIA: 28637
http://secunia.com/advisories/28637
* SECUNIA: 28739
http://secunia.com/advisories/28739
* SECUNIA: 28838
http://secunia.com/advisories/28838
* SECUNIA: 29706
http://secunia.com/advisories/29706
* XF: mysql-federated-engine-dos(38990)
http://xforce.iss.net/xforce/xfdb/38990

CVE Reference:

CVE-2007-6304 (cve.mitre.org, nvd.nist.gov)

• 13637 MySQL InnoDB engine, CONTAINS operation on an indexed column Denial of Service Vulnerability

The convert_search_mode_to_innobase function in ha_innodb.cc in the InnoDB engine in MySQL 5.1.23-BK and earlier allows remote authenticated users to cause a denial of service (database crash) via a certain CONTAINS operation on an indexed column, which triggers an assertion error.

The security issue has been reported in versions:
MySQL 5.0.x before 5.0.54, 5.1.x before 5.1.23, and 6.0.x before 6.0.4

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

References:

* CONFIRM:
http://bugs.mysql.com/bug.php?id=32125
* CONFIRM:

http://bugs.gentoo.org/show_bug.cgi?id=198988
* DEBIAN: DSA-1413
http://www.debian.org/security/2007/dsa-1413
* FEDORA: FEDORA-2007-4465
https://www.redhat.com/archives/fedora-package-announce/2007-December/msg00467.html
* FEDORA: FEDORA-2007-4471
https://www.redhat.com/archives/fedora-package-announce/2007-December/msg00475.html
* GENTOO: GLSA-200711-25
http://security.gentoo.org/glsa/glsa-200711-25.xml
* MANDRIVA: MDKSA-2007:243
http://www.mandriva.com/security/advisories?name=MDKSA-2007:243
* REDHAT: RHSA-2007:1155
http://www.redhat.com/support/errata/RHSA-2007-1155.html
* REDHAT: RHSA-2007:1157
http://www.redhat.com/support/errata/RHSA-2007-1157.html
* SLACKWARE: SSA:2007-348-01
http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.428959
* SUSE: SUSE-SR:2008:003
http://lists.opensuse.org/opensuse-security-announce/2008-02/msg00003.html
* UBUNTU: USN-559-1
http://www.ubuntulinux.org/support/documentation/usn/usn-559-1
* BID: 26353
http://www.securityfocus.com/bid/26353
* FRSIRT: ADV-2007-3903
http://www.frsirt.com/english/advisories/2007/3903
* SECTRACK: 1018978
http://www.securitytracker.com/id?1018978
* SECUNIA: 27568
http://secunia.com/advisories/27568
* SECUNIA: 27649
http://secunia.com/advisories/27649
* SECUNIA: 27823
http://secunia.com/advisories/27823
* SECUNIA: 28040
http://secunia.com/advisories/28040
* SECUNIA: 28025
http://secunia.com/advisories/28025
* SECUNIA: 28108
http://secunia.com/advisories/28108
* SECUNIA: 28099
http://secunia.com/advisories/28099
* SECUNIA: 28128
http://secunia.com/advisories/28128
* SECUNIA: 28838
http://secunia.com/advisories/28838
* XF: mysql-hainnodb-dos(38284)
http://xforce.iss.net/xforce/xfdb/38284

CVE Reference:

CVE-2007-5925 (cve.mitre.org, nvd.nist.gov)

- **13638 MySQL MyISAM table CREATE TABLE with modified DATA DIRECTORY or INDEX DIRECTORY arguments privilege checks bypass Vulnerability**

MySQL 4.1.x before 4.1.24, 5.0.x before 5.0.60, 5.1.x before 5.1.24, and 6.0.x before 6.0.5 allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are within the MySQL home data directory, which can point to tables that are created in the future.

The security issue has been reported in versions:
MySQL 4.1.x before 4.1.24, 5.0.x before 5.0.60, 5.1.x before 5.1.24, and 6.0.x before 6.0.5

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

References:

* CONFIRM:
http://bugs.mysql.com/bug.php?id=32167
* CONFIRM:
http://dev.mysql.com/doc/refman/4.1/en/news-4-1-24.html
* CONFIRM:
http://dev.mysql.com/doc/refman/5.0/en/releasenotes-es-5-0-60.html
* CONFIRM:
http://dev.mysql.com/doc/refman/5.1/en/news-5-1-24.html
* CONFIRM:
http://dev.mysql.com/doc/refman/6.0/en/news-6-0-5.html
* SECUNIA: 30134
http://secunia.com/advisories/30134

CVE Reference:

CVE-2008-2079 (cve.mitre.org, nvd.nist.gov)

- **13639 MySQL yaSSL Multiple buffer overflows arbitrary code execution Vulnerability**

Multiple buffer overflows in yaSSL 1.7.5 and earlier, as used in MySQL and possibly other products, allow remote attackers to execute arbitrary code via the ProcessOldClientHello function in handshake.cpp or "input_buffer& operator>>" in yassl_imp.cpp.

The security issue has been reported in versions:
MySQL 5.0.x before 5.0.58, 5.1.x before 5.1.24, and 6.0.x before 6.0.5

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

References:

* BUGTRAQ: 20080104 Multiple vulnerabilities in yaSSL 1.7.5
http://www.securityfocus.com/archive/1/archive/1/485810/100/0/threaded
* BUGTRAQ: 20080104 Pre-auth buffer-overflow in mySQL through yaSSL

http://www.securityfocus.com/archive/1/archive/1/485811/100/0/threaded
* CONFIRM:
http://bugs.mysql.com/33814
* CONFIRM:
http://dev.mysql.com/doc/refman/5.1/en/news-5-1-23.html
* DEBIAN: DSA-1478
http://www.debian.org/security/2008/dsa-1478
* UBUNTU: USN-588-1
http://www.ubuntu.com/usn/usn-588-1
* BID: 27140
http://www.securityfocus.com/bid/27140
* FRSIRT: ADV-2008-0560
http://www.frsirt.com/english/advisories/2008/0560/references
* SECUNIA: 28324
http://secunia.com/advisories/28324
* SECUNIA: 28419
http://secunia.com/advisories/28419
* SECUNIA: 28597
http://secunia.com/advisories/28597
* SECUNIA: 29443
http://secunia.com/advisories/29443
* SREASON: 3531
http://securityreason.com/securityalert/3531

CVE Reference:

CVE-2008-0226 (cve.mitre.org, nvd.nist.gov)

• 16920 Word Object Parsing Vulnerability (MS08-026/951207) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office handles specially crafted Rich Text Format (.rtf) files. The vulnerability could allow remote code execution if a user opens a specially crafted .rtf file with malformed strings in Word or previews a specially crafted .rtf file with malformed strings in rich text e-mail. 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.

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

References:

* MS: MS08-026
http://www.microsoft.com/technet/security/bulletin/ms08-026.mspx
* CERT-VN: VU#543907
http://www.kb.cert.org/vuls/id/543907
* FRSIRT: ADV-2008-1504
http://www.frsirt.com/english/advisories/2008/1504/references

CVE Reference:

CVE-2008-1091 (cve.mitre.org, nvd.nist.gov)

- **16921 Word Cascading Style Sheet (CSS) Vulnerability (MS08-026/951207) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Word handles specially crafted Word files. The vulnerability could allow remote code execution if a user opens a specially crafted Word file that includes a malformed CSS value. 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.

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

References:

* MS: MS08-026
http://www.microsoft.com/technet/security/bulletin/ms08-026.mspx
* FRSIRT: ADV-2008-1504
http://www.frsirt.com/english/advisories/2008/1504/references

CVE Reference:

CVE-2008-1434 (cve.mitre.org, nvd.nist.gov)

- **16922 Publisher Object Handler Validation Vulnerability (MS08-027/951208) (Remote File Checking)**

A remote code execution vulnerability exists in the way Microsoft Publisher validates object header data. An attacker could exploit the vulnerability by sending a specially crafted Publisher file which could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

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:

* MS: MS08-027
http://www.microsoft.com/technet/security/bulletin/ms08-027.mspx
* FRSIRT: ADV-2008-1505
http://www.frsirt.com/english/advisories/2008/1505/references
* SECUNIA: 30150
http://secunia.com/advisories/30150
* BID: 29158
http://www.securityfocus.com/bid/29158
* SECTRACK: 1020015
http://www.securitytracker.com/id?1020015

CVE Reference:

CVE-2008-0119 (cve.mitre.org, nvd.nist.gov)

- **16923 Microsoft Jet Engine MDB File Parsing Stack Overflow Vulnerability (MS08-028/950749) (Remote File Checking)**

A buffer overrun vulnerability exists in the Microsoft Jet Database Engine (Jet) that could allow remote code execution on an affected system. An attacker could exploit the vulnerability by creating a specially crafted database query and sending it through an application that is using Jet on an affected system. 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 impacted than users who operate with administrative user rights.

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

References:

* BUGTRAQ: 20071116 Microsoft Jet Engine MDB File Parsing Stack Overflow Vulnerability
http://www.securityfocus.com/archive/1/archive/1/483797/100/0/threaded
* BUGTRAQ: 20071116 Re: Microsoft Jet Engine MDB File Parsing Stack Overflow Vulnerability
http://www.securityfocus.com/archive/1/archive/1/483858/100/100/threaded
* BUGTRAQ: 20071117 Re: Microsoft Jet Engine MDB File Parsing Stack Overflow Vulnerability
http://www.securityfocus.com/archive/1/archive/1/483887/100/100/threaded
* BUGTRAQ: 20071118 Re: [Full-disclosure] Microsoft Jet Engine MDB File Parsing Stack Overflow Vulnerability
http://www.securityfocus.com/archive/1/archive/1/483888/100/100/threaded
* FULLDISC: 20071116 Microsoft Jet Engine MDB File Parsing Stack Overflow Vulnerability
http://lists.grok.org.uk/pipermail/full-disclosure/2007-November/058531.html
* MISC:
http://ruder.cdut.net/blogview.asp?logID=227
* CERT-VN: VU#936529
http://www.kb.cert.org/vuls/id/936529
* BID: 26468
http://www.securityfocus.com/bid/26468
* SECTRACK: 1018976
http://www.securitytracker.com/id?1018976
* SREASON: 3376
http://securityreason.com/securityalert/3376
* XF: microsoft-jet-engine-mdb-bo(38499)
http://xforce.iss.net/xforce/xfdb/38499
* MS: MS08-028
http://www.microsoft.com/technet/security/Bulletin/ms08-028.mspx

CVE Reference:

CVE-2007-6026 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

Microsoft Patch Tuesday

This Tuesday, Microsoft released patches for the below security issues.

- Word Cascading Style Sheet (CSS) Vulnerability (MS08-026/951207)
- Microsoft Jet Engine MDB File Parsing Stack Overflow Vulnerability (MS08-028/950749)
- Word Object Parsing Vulnerability (MS08-026/951207)
- Publisher Object Handler Validation Vulnerability (MS08-027/951208)
- Microsoft Malware Protection Engine Vulnerability (CVE-2008-1437) (MS08-029/952044)
- Microsoft Malware Protection Engine Vulnerability (CVE-2008-1438) (MS08-029/952044)

References:
http://www.microsoft.com/technet/security/bulletin/ms08-026.mspx
http://www.microsoft.com/technet/security/bulletin/ms08-027.mspx
http://www.microsoft.com/technet/security/bulletin/ms08-028.mspx
http://www.microsoft.com/technet/security/bulletin/ms08-029.mspx

Microsoft Windows CE Image Processing Vulnerabilities

"Execution of arbitrary code"

Some vulnerabilities have been reported in Microsoft Windows CE, which potentially can be exploited by malicious people to compromise a vulnerable system.

The vulnerabilities are caused due to unspecified errors when processing JPEG images (GDI+) and in the GIF imaging components. No more information is currently available.

Successful exploitation may allow execution of arbitrary code.

References:
http://support.microsoft.com/kb/948812

Microsoft Windows XP I2O Utility Filter Driver Privilege Escalation

"Gain escalated privileges"

A vulnerability has been reported in Microsoft Windows XP, which can be exploited by malicious, local users to gain escalated privileges.

An input validation error within a certain IOCTL handler in the I2O Utility Filter driver (i2omgmt.sys) and insecure permissions on the \\.\I2OExc device interface can be exploited to overwrite arbitrary memory and execute code with kernel privileges.

The vulnerability is reported in Windows XP SP2 including i2omgmt.sys version 5.1.2600.2180. Other versions may also be affected.

References:
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=699

Internet Explorer "Print Table of Links" Cross-Zone Scripting
"Execution of arbitrary code"

Aviv Raff has discovered a vulnerability in Internet Explorer, which can be exploited by malicious people to compromise a user's system.

Input passed via links within an HTML file is not being properly sanitized before being used to generate a printable HTML file. This can be exploited to inject arbitrary script code, which is executed in local context when a user is enticed to print a specially crafted HTML document with the "Print table of links" option enabled.

Successful exploitation allows execution of arbitrary code.

The vulnerability is confirmed in Internet Explorer 6 and 7 on a fully patched Windows XP SP2. Other versions may also be affected.

References:
http://aviv.raffon.net/2008/05/14/InternetExplorerQuotPrintTableOfLinksquotCrossZoneScriptingVulnerability.aspx

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