netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 27

July 4, 2008

Table of Contents

Product Focus

This Week in Review

Top Security News Stories this Week

New Vulnerabilities Tested in SecureScout

New Vulnerabilities found this Week

Product Focus

Messenger Service Vulnerability Scanner – The S4 Messenger Service 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 Microsoft Windows Messenger Service flaw (MS03-043).

The National Vulnerability Database (NVD) part of the National Institute of Standards and Technology (NIST) has recognized netVigilance for its detailed feedback on the NVD CVSS v2 scores. See http://www.netvigilance.com/press6-16-08

This week netVigilance Security Research has found 5 vulnerabilities in open source software Fa Name and myBloggie:
All medium risk with CVSS 2.0 base scores between 4.3 and 6.8. The vulnerabilities include SQL Injection, XSS (Cross site Scripting) and Path Disclosure Vulnerabilities.
For details and further information please see: http://www.netvigilance.com/advisories

This Week in Review

Happy 4rth of July, but be careful out there. PCI to cover unattended terminals. Microsoft tries to form new Industry Consortium for security. Now that is an idea: Best before date for browsers...

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

❖ 4th of July malware attack targets holidaying American computer users

Experts at SophosLabs™, Sophos's global network of virus, spyware and spam analysis centers, have warned of a widespread email spam campaign that poses as a video of American Independence Day fireworks, but is really attempt to lure innocent computer users into having their computers hacked. The attack is the latest from the gang behind the Dorf malware, also known as the Storm worm.

Sophos

Full Story :
http://www.sophos.com/pressoffice/news/articles/2008/07/july4.html?_log_from=rss

❖ PCI standard to include unattended POS

The PCI Security Standards Council this week said it will produce additional guidelines to cover unattended payment terminals, such as those found in vending machines and on fuel pumps.

Previously the guidelines only covered attended point-of-sale devices.

The additions mean extra requirements for retailers, which will now need to secure their systems not only in data centers and stores, but at all terminals where a PIN is entered.

Though the PCI Standards Council did not mention last year's hack on international retail giant TJX, which possibly started through a store kiosk, such incidents have raised concerns over the security of point-of-sale terminals.

SC Magazine

Full Story :
http://www.scmagazineus.com/PCI-standard-to-include-unattended-POS/article/112049/

❖ Microsoft presses deeper into security space

Microsoft is spearheading its second global security initiative in a week by setting up a scheme to try to tackle multi-vendor security threats.

The software giant is joining forces with Cisco, IBM, Intel and Juniper Networks, to form a "lean" organization called ICASI (Industry Consortium for Advancement of Security on the Internet).

ICASI's aim is to tackle security threats which affect multiple vendors' products, without having to involve government organizations. ICASI argues its creation is due to the fact that internet threats have evolved in complexity from simple worms and viruses to become sophisticated attacks across multiple products. Its board of directors will comprise one executive from each of the five vendors.

SC Magazine

Full Story :
http://www.scmagazineus.com/Microsoft-presses-deeper-into-security-space/article/111979/

- **Calls for 'best before' dates for browsers**

Because your IE6 is starting to smell funny...
A group of researchers has recommended that internet software, such as browsers should come with a 'best before' date to keep users safe from malware and hackers.

A staggering 41% of internet users do not use the latest version of their browser, leaving themselves at risk from hackers who use exploits in the software to gain entry to their computers.

Thestudy suggested that, of the 1,408 million internet users, 576 million 'surfed the internet without using the latest major browser version of their preferred browser.'

Tech radar

Full Story :
http://www.techradar.com/news/software/calls-for-best-before-dates-for-browsers-416243

New Vulnerabilities Tested in SecureScout

- **13641 Skype File URI Security Bypass Code Execution Vulnerability (CVE-2008-2545) (Remote File Checking)**

  Skype is a free program that uses the latest P2P (cutting edge p2p technology) technology to bring affordable and high-quality voice communications.

  Remote exploitation of a security policy bypass in Windows Skype versions could allow an attacker to execute arbitrary code.

URI handler in Skype performs checks upon the URL to verify that the link does not contain certain file extensions related to executable file formats. If the link is found to contain a blacklisted executable file extension a security warning dialog is shown to the user. The check is performed using the case sensitive comparison.

All releases prior to and including 3.8.*.115 are affected.

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

References:

* IDEFENSE: 20080604 Skype File URI Security Bypass Code Execution Vulnerability
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=711
* CONFIRM:
http://www.skype.com/security/skype-sb-2008-003.html
* BID: 29553
http://www.securityfocus.com/bid/29553
* FRSIRT: ADV-2008-1749
http://www.frsirt.com/english/advisories/2008/1749/references
* SECTRACK: 1020201
http://www.securitytracker.com/id?1020201
* SECUNIA: 30547
http://secunia.com/advisories/30547

CVE Reference:

CVE-2008-2545 (cve.mitre.org, nvd.nist.gov)

- **13642 Skype File URI Security Bypass Code Execution Vulnerability (CVE-2008-1805) (Remote File Checking)**

Skype is a free program that uses the latest P2P (cutting edge p2p technology) technology to bring affordable and high-quality voice communications.

Remote exploitation of a security policy bypass in Windows Skype versions could allow an attacker to execute arbitrary code.

URI handler in Skype performs checks upon the URL to verify that the link does not contain certain file extensions related to executable file formats. If the link is found to contain a blacklisted executable file extension a security warning dialog is shown to the user. The check is that the blacklist fails to mention all potential executable file formats. This allows an attacker to bypass this security policy and execute arbitrary code if a victim clicks an attacker supplied URL.

All releases prior to and including 3.8.*.115 are affected.

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

References:

* IDEFENSE: 20080604 Skype File URI Security Bypass Code Execution Vulnerability
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=711
* CONFIRM:

http://www.skype.com/security/skype-sb-2008-003.html
* BID: 29553
http://www.securityfocus.com/bid/29553
* FRSIRT: ADV-2008-1749
http://www.frsirt.com/english/advisories/2008/1749/references
* SECTRACK: 1020201
http://www.securitytracker.com/id?1020201
* SECUNIA: 30547
http://secunia.com/advisories/30547

CVE Reference:

CVE-2008-1805 (cve.mitre.org, nvd.nist.gov)

- **13643 Skype Improper handling of URI arguments (CVE-2007-5989) (Remote File Checking)**

Skype is a free program that uses the latest P2P (cutting edge p2p technology) technology to bring affordable and high-quality voice communications.

The flaw exists within the skype4com URI handler component of Skype. An exploitable memory corruption may occur during the parsing of URIs which can result in arbitrary code execution under the user rights of the current Windows account.

An attacker who constructs a Skype URI that is malformed in a specific way can cause Skype to crash and allow for the execution of arbitrary instructions. For the vulnerability to be triggered, the target must visit a malicious web page.

This behavior is due to incorrect handling of arguments passed to a function in the Skype skype4com URI handler.

All releases prior to and including 3.6.*.196 are affected.

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

References:

* BUGTRAQ: 20071206 ZDI-07-070: Skype skype4com URI Handler Remote Heap Corruption Vulnerability
http://www.securityfocus.com/archive/1/archive/1/484703/100/0/threaded
* MISC:
http://www.zerodayinitiative.com/advisories/ZDI-07-070.html
* BID: 26748
http://www.securityfocus.com/bid/26748
* FRSIRT: ADV-2007-4110
http://www.frsirt.com/english/advisories/2007/4110
* SECTRACK: 1019056
http://securitytracker.com/id?1019056
* SECUNIA: 27934
http://secunia.com/advisories/27934
* SREASON: 3440
http://securityreason.com/securityalert/3440

CVE Reference:

CVE-2007-5989 (cve.mitre.org, nvd.nist.gov)

- **13644 Skype Improper handling of URI arguments (CVE-2007-3896) (Remote File Checking)**

Skype is a free program that uses the latest P2P (cutting edge p2p technology) technology to bring affordable and high-quality voice communications.

In some circumstances, a Skype URI can be crafted that, if followed, an executable accessible with the current Windows user rights is launched.

An attacker who constructs a Skype URI that is malformed in a specific way can execute programs which are accessible for current Windows user.
For the vulnerability to be triggered, the target must click on a link in the chat, mood message or visit maliciously crafted web page.

The URL handling in Shell32.dll in the Windows shell in Microsoft Windows XP and Server 2003, with Internet Explorer 7 installed, allows remote attackers to execute arbitrary programs via invalid "%" sequences in a mailto: or other URI handler, as demonstrated using mIRC, Outlook, Firefox, Adobe Reader, Skype, and other applications.

All releases prior to and including 3.5.*.236 are affected.

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

References:

* BUGTRAQ: 20071011 M$ will fix URI?
http://www.securityfocus.com/archive/1/archive/1/482090/100/0/threaded
* BUGTRAQ: 20071014 Third-party patch for CVE-2007-3896 (Internet Explorer 7 invalid URI handling) available
http://www.securityfocus.com/archive/1/archive/1/482292/100/0/threaded
* BUGTRAQ: 20071017 Re: Third-party patch for CVE-2007-3896, UPDATE NOW
http://www.securityfocus.com/archive/1/archive/1/482437/100/0/threaded
* BUGTRAQ: 20071004 Re: 0day: mIRC pwns Windows
http://www.securityfocus.com/archive/1/archive/1/481505/100/0/threaded
* BUGTRAQ: 20071004 Re[2]: 0day: mIRC pwns Windows
http://www.securityfocus.com/archive/1/archive/1/481493/100/100/threaded
* BUGTRAQ: 20071005 RE: URI handling woes in Acrobat Reader, Netscape, Miranda, Skype
http://www.securityfocus.com/archive/1/archive/1/481624/100/0/threaded
* BUGTRAQ: 20071006 Re[2]: URI handling woes in Acrobat Reader, Netscape, Miranda, Skype
http://www.securityfocus.com/archive/1/archive/1/481664/100/0/threaded
* BUGTRAQ: 20071006 Re[2]: [Full-disclosure] URI handling woes in Acrobat Reader, Netscape, Miranda, Skype
http://www.securityfocus.com/archive/1/archive/1/481671/100/0/threaded
* BUGTRAQ: 20071006 Re[2]: [Full-disclosure] URI handling woes in Acrobat Reader, Netscape,Miranda, Skype
http://www.securityfocus.com/archive/1/archive/1/481680/100/0/threaded
* BUGTRAQ: 20071007 Re: Re[2]: [Full-disclosure] URI handling woes in Acrobat

Reader, Netscape,Miranda, Skype
http://www.securityfocus.com/archive/1/archive/1/481881/100/0/threaded
* BUGTRAQ: 20071007 Re: [Full-disclosure] URI handling woes in Acrobat Reader, Netscape,Miranda, Skype
http://www.securityfocus.com/archive/1/archive/1/481846/100/0/threaded
* BUGTRAQ: 20071007 Re[2]: [Full-disclosure] URI handling woes in Acrobat Reader, Netscape, Miranda, Skype
http://www.securityfocus.com/archive/1/archive/1/481839/100/0/threaded
* BUGTRAQ: 20071008 Re: [Full-disclosure] URI handling woes in Acrobat Reader, Netscape, Miranda, Skype
http://www.securityfocus.com/archive/1/archive/1/481887/100/0/threaded
* BUGTRAQ: 20071008 Re: [Full-disclosure] URI handling woes in Acrobat Reader, Netscape,Miranda, Skype
http://www.securityfocus.com/archive/1/archive/1/481867/100/0/threaded
* BUGTRAQ: 20071009 RE: [Full-disclosure] URI handling woes in Acrobat Reader, Netscape, Miranda, Skype
http://www.securityfocus.com/archive/1/archive/1/481871/100/0/threaded
* MISC:
http://blogs.zdnet.com/security/?p=577
* MISC:
http://www.heise-security.co.uk/news/96982
* MISC:
http://xs-sniper.com/blog/remote-command-exec-firefox-2005/
* BUGTRAQ: 20071003 0day: mIRC pwns Windows
http://marc.info/?l=bugtraq&m=119143780202107&w=2
* BUGTRAQ: 20071003 Re: 0day: mIRC pwns Windows
http://marc.info/?l=bugtraq&m=119144449915918&w=2
* BUGTRAQ: 20071005 URI handling woes in Acrobat Reader, Netscape, Miranda, Skype
http://marc.info/?l=bugtraq&m=119159924712561&w=2
* BUGTRAQ: 20071006 Re: URI handling woes in Acrobat Reader, Netscape, Miranda, Skype
http://marc.info/?l=bugtraq&m=119168062128026&w=2
* BUGTRAQ: 20071007 Re: [Full-disclosure] URI handling woes in Acrobat Reader, Netscape, Miranda, Skype
http://marc.info/?l=bugtraq&m=119195904813505&w=2
* BUGTRAQ: 20071009 Re: URI handling woes in Acrobat Reader, Netscape, Miranda, Skype
http://marc.info/?l=bugtraq&m=119194714125580&w=2
* FULLDISC: 20071006 Re: URI handling woes in Acrobat Reader, Netscape, Miranda, Skype
http://marc.info/?l=full-disclosure&m=119171444628628&w=2
* FULLDISC: 20071005 URI handling woes in Acrobat Reader, Netscape, Miranda, Skype
http://marc.info/?l=full-disclosure&m=119159477404263&w=2
* FULLDISC: 20071006 Re: URI handling woes in Acrobat Reader, Netscape, Miranda, Skype
http://marc.info/?l=full-disclosure&m=119168727402084&w=2
* FULLDISC: 20071006 Re: URI handling woes in Acrobat Reader, Netscape, Miranda, Skype
http://marc.info/?l=full-disclosure&m=119170531020020&w=2
* FULLDISC: 20071007 Re: URI handling woes in Acrobat Reader, Netscape, Miranda, Skype
http://marc.info/?l=full-disclosure&m=119175323322021&w=2
* FULLDISC: 20071007 Re: URI handling woes in Acrobat Reader, Netscape,

Miranda, Skype
http://marc.info/?l=full-disclosure&m=119180333805950&w=2
* HP: HPSBST02291
http://www.securityfocus.com/archive/1/archive/1/484186/100/0/threaded
* MS: MS07-061
http://www.microsoft.com/technet/security/bulletin/MS07-061.mspx
* MSKB: 943521
http://www.microsoft.com/technet/security/advisory/943521.mspx
* CERT: TA07-317A
http://www.us-cert.gov/cas/techalerts/TA07-317A.html
* CERT-VN: VU#403150
http://www.kb.cert.org/vuls/id/403150
* BID: 25945
http://www.securityfocus.com/bid/25945
* OVAL: oval:org.mitre.oval:def:4581
http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4581
* SECTRACK: 1018822
http://www.securitytracker.com/id?1018822
* SECTRACK: 1018831
http://securitytracker.com/id?1018831
* SECUNIA: 26201
http://secunia.com/advisories/26201

CVE Reference:

CVE-2007-3896 (cve.mitre.org, nvd.nist.gov)

- **13646 Skype callto handling range check error (Remote File Checking)**

Skype is a free program that uses the latest P2P (cutting edge p2p technology) technology to bring affordable and high-quality voice communications.

A range check error exists in the way Skype parses command-line arguments. If Skype is executed with a command line longer than approximately 4096 characters, Skype would report an Access Violation and terminate.

The vulnerability can not be used for malicious code execution.

All releases prior to 0.98.0.28 are affected.

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

References:

* BUGTRAQ: 20040615 Skype URI callto username overflow
http://lists.virus.org/bugtraq-0406/msg00221.html
* CONFIRM:
http://www.skype.com/security/ssa-2004-01.html
* OSVDB: 11860
http://www.osvdb.org/11860
* SECTRACK: 1010490
http://securitytracker.com/id?1010490

CVE Reference:

CVE-2004-1777 (cve.mitre.org, nvd.nist.gov)

- **16975 Wireshark GSM SMS dissector denial of service Vulnerability (Remote File Checking)**

A vulnerability in the GSM SMS dissector in Wireshark (formerly Ethereal) 0.99.2 to 1.0.0 allows remote attackers to cause a denial of service (application crash).

The vulnerability is reported in versions 0.99.2 to 1.0.0.

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

References:

* CONFIRM: wnpa-sec-2008-03
http://www.wireshark.org/security/wnpa-sec-2008-03.html
* SECUNIA: SA30886
http://secunia.com/advisories/30886/
* SECTRACK: 1020404
http://www.securitytracker.com/alerts/2008/Jul/1020404.html
* FRSIRT: FrSIRT/ADV-2008-1982
http://www.frsirt.com/english/advisories/2008/1982/references
* BID: 30020
http://www.securityfocus.com/bid/30020

CVE Reference:

- **16976 Wireshark PANA and KISMET dissectors denial of service Vulnerability (Remote File Checking)**

A vulnerability in the PANA and KISMET dissectors in Wireshark (formerly Ethereal) 0.99.3 to 1.0.0 allows remote attackers to cause a denial of service (application crash).

The vulnerability is reported in versions 0.99.3 to 1.0.0.

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

References:

* CONFIRM: wnpa-sec-2008-03
http://www.wireshark.org/security/wnpa-sec-2008-03.html
* SECUNIA: SA30886
http://secunia.com/advisories/30886/
* SECTRACK: 1020404
http://www.securitytracker.com/alerts/2008/Jul/1020404.html
* FRSIRT: FrSIRT/ADV-2008-1982
http://www.frsirt.com/english/advisories/2008/1982/references
* BID: 30020
http://www.securityfocus.com/bid/30020

CVE Reference:

- **16977 Wireshark RTMPT dissector denial of service Vulnerability (Remote File Checking)**

A vulnerability in the RTMPT dissector in Wireshark (formerly Ethereal) 0.99.8 to 1.0.0 allows remote attackers to cause a denial of service (application crash).

The vulnerability is reported in versions 0.99.8 to 1.0.0.

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

References:

* CONFIRM: wnpa-sec-2008-03
http://www.wireshark.org/security/wnpa-sec-2008-03.html
* SECUNIA: SA30886
http://secunia.com/advisories/30886/
* SECTRACK: 1020404
http://www.securitytracker.com/alerts/2008/Jul/1020404.html
* FRSIRT: FrSIRT/ADV-2008-1982
http://www.frsirt.com/english/advisories/2008/1982/references
* BID: 30020
http://www.securityfocus.com/bid/30020

CVE Reference:

- **16978 Wireshark RMI dissector information disclosure Vulnerability (Remote File Checking)**

An information disclosure vulnerability in the RMI dissector in Wireshark (formerly Ethereal) 0.9.5 to 1.0.0 allows remote attackers to disclose system memory.

The vulnerability is reported in versions 0.9.5 to 1.0.0.

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

References:

* CONFIRM: wnpa-sec-2008-03
http://www.wireshark.org/security/wnpa-sec-2008-03.html
* SECUNIA: SA30886
http://secunia.com/advisories/30886/
* SECTRACK: 1020404
http://www.securitytracker.com/alerts/2008/Jul/1020404.html
* FRSIRT: FrSIRT/ADV-2008-1982
http://www.frsirt.com/english/advisories/2008/1982/references
* BID: 30020
http://www.securityfocus.com/bid/30020

CVE Reference:

- **16979 Wireshark syslog dissector denial of service Vulnerability (Remote File Checking)**

A vulnerability in the syslog dissector in Wireshark (formerly Ethereal) 1.0.0 allows remote attackers to cause a denial of service (application crash).

The vulnerability is reported in version 1.0.0.

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

References:

* CONFIRM: wnpa-sec-2008-03
http://www.wireshark.org/security/wnpa-sec-2008-03.html
* SECUNIA: SA30886
http://secunia.com/advisories/30886/
* SECTRACK: 1020404
http://www.securitytracker.com/alerts/2008/Jul/1020404.html
* FRSIRT: FrSIRT/ADV-2008-1982
http://www.frsirt.com/english/advisories/2008/1982/references
* BID: 30020
http://www.securityfocus.com/bid/30020

CVE Reference:

New Vulnerabilities found this Week

- **CVE-2008-2959 Microsoft CVSS 2.0 Score = 9.3**

Buffer overflow in a certain ActiveX control (vb6skit.dll) in Microsoft Visual Basic Enterprise Edition 6.0 SP6 might allow remote attackers to execute arbitrary code via a long lpstrLinkPath argument to the fCreateShellLink function.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

MILW0RM: http://www.milw0rm.com/exploits/5851

BID: http://www.securityfocus.com/bid/29792

XF: http://xforce.iss.net/xforce/xfdb/43180

CVE Reference: CVE-2008-2959

- **CVE-2008-2947 Microsoft CVSS 2.0 Score = 6.8**

Cross-domain vulnerability in Microsoft Internet Explorer 6 allows remote attackers to access restricted information from other domains via JavaScript that uses the Object data type for the value of a (1) location or (2) location.href property.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

http://blogs.zdnet.com/security/?p=1348

http://www.ph4nt0m.org-a.googlepages.com/PSTZine_0x02_0x04.txt

CERT-VN: http://www.kb.cert.org/vuls/id/923508

BID: http://www.securityfocus.com/bid/29960

FRSIRT: http://www.frsirt.com/english/advisories/2008/1940/references

SECUNIA: http://secunia.com/advisories/30857

XF: http://xforce.iss.net/xforce/xfdb/43366

CVE Reference: CVE-2008-2947

- **CVE-2008-2948 Microsoft CVSS 2.0 Score = 6.8**

Cross-domain vulnerability in Microsoft Internet Explorer 7 and 8 allows remote attackers to change the location property of a frame via the Object data type, and use a frame from a different domain to observe domain-independent events, as demonstrated by observing onkeydown events with caballero-listener.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

http://blogs.zdnet.com/security/?p=1348

http://sirdarckcat.blogspot.com/2008/05/ghosts-for-ie8-and-ie75730.html

http://technet.microsoft.com/en-us/security/cc405107.aspx#EHD

http://www.gnucitizen.org/blog/ghost-busters/

CERT-VN: http://www.kb.cert.org/vuls/id/516627

FRSIRT: http://www.frsirt.com/english/advisories/2008/1941/references

SECUNIA: http://secunia.com/advisories/30851

CVE Reference: CVE-2008-2948

- **CVE-2008-2949 Microsoft CVSS 2.0 Score = 6.8**

Cross-domain vulnerability in Microsoft Internet Explorer 6 and 7 allows remote attackers to change the location property of a frame via the String data type, and use a frame from a different domain to observe domain-independent events, as demonstrated by observing onkeydown events with caballero-listener.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

http://blogs.zdnet.com/security/?p=1348

http://sirdarckcat.blogspot.com/2008/05/browsers-ghost-busters.html

http://technet.microsoft.com/en-us/security/cc405107.aspx#EHD

CERT-VN: http://www.kb.cert.org/vuls/id/516627

FRSIRT: http://www.frsirt.com/english/advisories/2008/1941/references

CVE Reference: CVE-2008-2949

- **CVE-2008-2943 IBM CVSS 2.0 Score = 6.0**

Double free vulnerability in IBM Tivoli Directory Server (TDS) 6.1.0.0 through 6.1.0.15 allows remote authenticated administrators to cause a denial of service (ABEND) and possibly execute arbitrary code by using ldapadd to attempt to create a duplicate ibm-globalAdminGroup LDAP database entry. NOTE: the vendor states "There is no real risk of a vulnerability," although there are likely scenarios in which a user is allowed to make administrative LDAP requests but does not have the privileges to stop the server.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

AIXAPAR: http://www-1.ibm.com/support/docview.wss?uid=swg1IO09113

FRSIRT: http://www.frsirt.com/english/advisories/2008/1970

SECUNIA: http://secunia.com/advisories/30786

CVE Reference: CVE-2008-2943

- **CVE-2008-2908 Novell CVSS 2.0 Score = 9.3**

Multiple stack-based buffer overflows in a certain ActiveX control in ienipp.ocx in Novell iPrint Client for Windows before 4.36 allow remote attackers to execute arbitrary code via a long value of the (1) operation, (2) printer-url, or (3) target-frame parameter. NOTE: some of these details are obtained from third party information.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

http://support.novell.com/docs/Readmes/InfoDocument/patchbuilder/readme_5028061.html

CERT-VN: http://www.kb.cert.org/vuls/id/145313

FRSIRT: http://www.frsirt.com/english/advisories/2008/1837/references

SECUNIA: http://secunia.com/advisories/30709

CVE Reference: CVE-2008-2908

- **CVE-2008-2954 Linux CVSS 2.0 Score = 7.8**

client/NmdcHub.cpp in Linux DC++ (linuxdcpp) before 0.707 allows remote attackers to cause a denial of service (crash) via an empty private message, which triggers an out-of-bounds read.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

http://cvs.berlios.de/cgi-bin/viewcvs.cgi/linuxdcpp/linuxdcpp/Changelog.txt

http://cvs.berlios.de/cgi-bin/viewcvs.cgi/linuxdcpp/linuxdcpp/client/NmdcHub.cpp.diff?r1=1.14&r2=1.15&sortby=date

CVE Reference: CVE-2008-2954

- **CVE-2008-2946 Sun CVSS 2.0 Score = 7.8**

The SNMP-DMI mapper subagent daemon (aka snmpXdmid) in Solstice Enterprise Agents in Sun Solaris 8 through 10 allows remote attackers to cause a denial of service (daemon crash) via malformed packets.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

SUNALERT: http://sunsolve.sun.com/search/document.do?assetkey=1-26-237985-1

BID: http://www.securityfocus.com/bid/29965

SECUNIA: http://secunia.com/advisories/30863

CVE Reference: CVE-2008-2946

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