netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 28

July 11, 2008

Table of Contents

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).

This Week in Review

Serious dns-bug found. ICANN under attack. Wireless very popular amongst government employees. New technologies used by criminals.

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

- **Multiple vendors cooperate to issue DNS design flaw fix**

A massive domain name system (DNS) design vulnerability that could permit cache poisoning - effectively allowing an attacker to direct users to the website of his choosing - is set to be fixed by an unprecedented synchronized series of multivendor

patches.

The bug, discovered accidentally by researcher and DNS expert Dan Kaminsky, relates to deficiencies in the DNS protocol, a critical component of internet infrastructure that translates domain names into IP addresses and vice versa, essentially acting as the web"s phone book.

Kaminsky, director of penetration testing at IOActive, declined during a conference call on Tuesday to release specifics, noting that he plans to fully detail the flaw Aug. 6 and 7 at the Black Hat conference in Las Vegas.

SC Magazine

Full Story :
http://www.scmagazineus.com/Multiple-vendors-cooperate-to-issue-DNS-design-flaw-fix/article/112174/

❖ ICANN downplays site hacks

Hackers compromised a pair of mirror sites for the Internet Corporation of Assigned Names and Numbers (ICANN) and redirected users to a page taunting the company and claiming "we control the domains."

The attacks were attributed to Turkish hacker group NetDevilz.

The attack was particularly embarrassing for ICANN as it came just days after the group approved a plan to open new domains for registration by the public.

SC Magazine

Full Story :
http://www.scmagazineus.com/ICANN-downplays-site-hacks/article/112139/

❖ Survey says: Government employees enjoy wireless internet

Nearly half of all federal government employees use wireless internet that allows them to work outside the office, according to a survey commissioned by Telework Exchange, a public-private organization.

In addition, 83 percent of government IT executives found that wireless internet access can be used securely, and government agencies are backing that up by providing wireless security tools.

The "Federal Mobility 2.0" study, underwritten by Sprint, surveyed 150 federal IT professionals and 160 federal workers/teleworkers.

SC Magazine

Full Story :
http://www.scmagazineus.com/Survey-says-Government-employees-enjoy-wireless-internet/article/112175/

❖ Cybercriminals move with the times

Cybercrooks are using new technologies and reinventing forms of social engineering to ensnare consumers and businesses, security experts warn.

Trend Micro"s latest "Threat Roundup and Forecast 1H 2008" report found an upswing in web threats, but a steady decrease in adware and spyware generated by outdated methods which can no longer compete with high-level security.

Social engineering tactics such as the Nigerian phishing scam have been around for years, and cybercriminals continue to refresh and modernize this form of trickery based on the latest trends.

SC Magazine

Full Story :
http://www.scmagazineus.com/Cybercriminals-move-with-the-times/article/112216/

New Vulnerabilities Tested in SecureScout

- **16980 Microsoft DNS Insufficient Socket Entropy Vulnerability (MS08-037/953230) (Remote File Checking)**

A spoofing vulnerability exists in Windows DNS client and Windows DNS server. This vulnerability could allow a remote unauthenticated attacker to quickly and reliably spoof responses and insert records into the DNS server or client cache, thereby redirecting Internet traffic.

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

References:

* CISCO: 20080708 Multiple Cisco Products Vulnerable to DNS Cache Poisoning Attacks
http://www.cisco.com/en/US/products/products_security_advisory09186a00809c2168.shtml
* DEBIAN: DSA-1603
http://www.debian.org/security/2008/dsa-1603
* DEBIAN: DSA-1604
http://www.debian.org/security/2008/dsa-1604
* DEBIAN: DSA-1605
http://www.debian.org/security/2008/dsa-1605
* MS: MS08-037
http://www.microsoft.com/technet/security/bulletin/ms08-037.mspx
* UBUNTU: USN-622-1
http://www.ubuntu.com/usn/usn-622-1
* CERT: TA08-190B
http://www.us-cert.gov/cas/techalerts/TA08-190B.html

* CERT-VN: VU#800113
http://www.kb.cert.org/vuls/id/800113
* SECTRACK: 1020438
http://www.securitytracker.com/id?1020438
* SECTRACK: 1020440
http://www.securitytracker.com/id?1020440
* XF: win-dns-client-server-spoofing(43334)
http://xforce.iss.net/xforce/xfdb/43334

CVE Reference:

CVE-2008-1447 (cve.mitre.org, nvd.nist.gov)

- **16981 Microsoft DNS Cache Poisoning Vulnerability (MS08-037/953230) (Remote File Checking)**

A cache poisoning vulnerability exists in Windows DNS Server. The vulnerability could allow an unauthenticated remote attacker to send specially crafted responses to DNS requests made by vulnerable systems, thereby poisoning the DNS cache and redirecting Internet traffic from legitimate locations.

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

References:

* MS: MS08-037
http://www.microsoft.com/technet/security/bulletin/ms08-037.mspx
* SECUNIA: 30925
http://secunia.com/advisories/30925/
* FRSIRT: FrSIRT/ADV-2008-2019
http://www.frsirt.com/english/advisories/2008/2019
* SECTRACK: 1020437
http://www.securitytracker.com/alerts/2008/Jul/1020437.html
* BID: 30132
http://www.securityfocus.com/bid/30132

CVE Reference:

CVE-2008-1454 (cve.mitre.org, nvd.nist.gov)

- **16983 Outlook Web Access for Exchange Server Data Validation Cross-Site Scripting Vulnerability (MS08-039/953747) (Remote File Checking)**

This is a cross-site scripting vulnerability in the affected versions of Outlook Web Access (OWA) for Exchange Server. Exploitation of the vulnerability could lead to elevation of privilege on individual OWA clients connecting to Outlook Web Access for Exchange Server. To exploit the vulnerability, an attacker would have to convince a user to open a specially crafted e-mail that would run malicious script from within an individual OWA client. If the malicious script is executed, the script would run in the security context of the userâ's OWA session and could perform any action the user could perform such as reading, sending, and deleting e-mail as the logged-on user.

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

References:

* MS: MS08-039
http://www.microsoft.com/technet/security/bulletin/ms08-039.mspx
* SECTRACK: 1020439
http://www.securitytracker.com/id?1020439
* SECUNIA: 30964
http://secunia.com/advisories/30964
* XF: exchange-owa-email-fields-xss(43328)
http://xforce.iss.net/xforce/xfdb/43328
* BID: 30130
http://www.securityfocus.com/bid/30130

CVE Reference:

CVE-2008-2247 (cve.mitre.org, nvd.nist.gov)

• 16984 Outlook Web Access for Exchange Server HTML Parsing Cross-Site Scripting Vulnerability (MS08-039/953747) (Remote File Checking)

This is a cross-site scripting vulnerability in the affected versions of Outlook Web Access (OWA) for Exchange Server. Exploitation of the vulnerability could lead to elevation of privilege on individual OWA clients connecting to Outlook Web Access for Exchange Server. To exploit the vulnerability an attacker would have to convince a user to open a specially crafted e-mail that would run malicious script from within an individual OWA client. The script would run in the security context of the userâ's OWA session and could perform any action the user could perform, such as reading, sending, and deleting e-mail as the logged-on user.

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

References:

* MS: MS08-039
http://www.microsoft.com/technet/security/bulletin/ms08-039.mspx
* SECTRACK: 1020439
http://www.securitytracker.com/id?1020439
* SECUNIA: 30964
http://secunia.com/advisories/30964
* XF: exchange-owa-html-xss(43329)
http://xforce.iss.net/xforce/xfdb/43329

CVE Reference:

CVE-2008-2248 (cve.mitre.org, nvd.nist.gov)

• 16985 SQL Server Memory Page Reuse Vulnerability (MS08-040/941203) (Remote File Checking)

An information disclosure vulnerability exists in the way that SQL Server manages memory page reuse. An attacker with database operator access who successfully exploited this vulnerability could access customer data.

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

References:

* MS: MS08-040
http://www.microsoft.com/technet/security/bulletin/ms08-040.mspx
* SECUNIA: 30970
http://secunia.com/advisories/30970/
* FRSIRT: FrSIRT/ADV-2008-2022
http://www.frsirt.com/english/advisories/2008/2022
* SECTRACK: 1020441
http://www.securitytracker.com/alerts/2008/Jul/1020441.html

CVE Reference:

CVE-2008-0085 (cve.mitre.org, nvd.nist.gov)

• 16986 SQL Server Convert Buffer Overrun (MS08-040/941203) (Remote File Checking)

A vulnerability exists in the convert function in SQL Server that could allow an authenticated attacker to gain elevation of privilege. An attacker who successfully exploited this vulnerability could run code and take complete control of the system.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **Medium**

References:

* SECUNIA: 30970
http://secunia.com/advisories/30970/
* FRSIRT: FrSIRT/ADV-2008-2022
http://www.frsirt.com/english/advisories/2008/2022
* SECTRACK: 1020441
http://www.securitytracker.com/alerts/2008/Jul/1020441.html
* MS: MS08-040
http://www.microsoft.com/technet/security/bulletin/ms08-040.mspx

CVE Reference:

CVE-2008-0086 (cve.mitre.org, nvd.nist.gov)

• 16987 SQL Server Memory Corruption Vulnerability (MS08-040/941203) (Remote File Checking)

A vulnerability exists in SQL Server that could allow an authenticated attacker to gain elevation of privilege. An attacker who successfully exploited this vulnerability could run code and take complete control of the system.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **Medium**

References:

* SECUNIA: 30970
http://secunia.com/advisories/30970/
* FRSIRT: FrSIRT/ADV-2008-2022
http://www.frsirt.com/english/advisories/2008/2022
* SECTRACK: 1020441
http://www.securitytracker.com/alerts/2008/Jul/1020441.html
* MS: MS08-040
http://www.microsoft.com/technet/security/bulletin/ms08-040.mspx

CVE Reference:

CVE-2008-0107 (cve.mitre.org, nvd.nist.gov)

- **16988 SQL Server Buffer Overrun Vulnerability (MS08-040/941203) (Remote File Checking)**

A vulnerability exists in SQL Server that could allow an authenticated attacker to gain elevation of privilege. An attacker who successfully exploited this vulnerability could run code and take complete control of the system.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **Medium**

References:

* SECUNIA: 30970
http://secunia.com/advisories/30970/
* FRSIRT: FrSIRT/ADV-2008-2022
http://www.frsirt.com/english/advisories/2008/2022
* SECTRACK: 1020441
http://www.securitytracker.com/alerts/2008/Jul/1020441.html
* MS: MS08-040
http://www.microsoft.com/technet/security/bulletin/ms08-040.mspx

CVE Reference:

CVE-2008-0106 (cve.mitre.org, nvd.nist.gov)

- **16989 BIND Insufficient Socket Entropy Vulnerability**

The DNS protocol, as implemented in BIND, Microsoft DNS and other implementations allow remote attackers to spoof DNS traffic via certain cache poisoning techniques against recursive resolvers, related to insufficient randomness of DNS transaction IDs and source ports, aka "DNS Insufficient Socket Entropy Vulnerability."

The vulnerability has been fixed in versions 9.5.0-P1, 9.4.2-P1, 9.3.5-P1.

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

References:

* CISCO: 20080708 Multiple Cisco Products Vulnerable to DNS Cache Poisoning Attacks
http://www.cisco.com/en/US/products/products_security_advisory09186a00809c2168.shtml
* DEBIAN: DSA-1603
http://www.debian.org/security/2008/dsa-1603
* DEBIAN: DSA-1604
http://www.debian.org/security/2008/dsa-1604
* DEBIAN: DSA-1605
http://www.debian.org/security/2008/dsa-1605
* MS: MS08-037
http://www.microsoft.com/technet/security/bulletin/ms08-037.mspx
* UBUNTU: USN-622-1
http://www.ubuntu.com/usn/usn-622-1
* CERT: TA08-190B
http://www.us-cert.gov/cas/techalerts/TA08-190B.html
* CERT-VN: VU#800113
http://www.kb.cert.org/vuls/id/800113
* SECTRACK: 1020438
http://www.securitytracker.com/id?1020438
* SECTRACK: 1020440
http://www.securitytracker.com/id?1020440
* XF: win-dns-client-server-spoofing(43334)
http://xforce.iss.net/xforce/xfdb/43334

CVE Reference:

CVE-2008-1447 (cve.mitre.org, nvd.nist.gov)

- **16990 Multiple Cisco Products Vulnerable to DNS Cache Poisoning Attacks (cisco-sa-20080708-dns)**

The DNS protocol, as implemented in BIND, Microsoft DNS and other implementations allow remote attackers to spoof DNS traffic via certain cache poisoning techniques against recursive resolvers, related to insufficient randomness of DNS transaction IDs and source ports, aka "DNS Insufficient Socket Entropy Vulnerability."

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

References:

* CISCO: 20080708 Multiple Cisco Products Vulnerable to DNS Cache Poisoning Attacks
http://www.cisco.com/en/US/products/products_security_advisory09186a00809c2168.shtml
* DEBIAN: DSA-1603
http://www.debian.org/security/2008/dsa-1603
* DEBIAN: DSA-1604
http://www.debian.org/security/2008/dsa-1604
* DEBIAN: DSA-1605
http://www.debian.org/security/2008/dsa-1605

* MS: MS08-037
http://www.microsoft.com/technet/security/bulletin/ms08-037.mspx
* UBUNTU: USN-622-1
http://www.ubuntu.com/usn/usn-622-1
* CERT: TA08-190B
http://www.us-cert.gov/cas/techalerts/TA08-190B.html
* CERT-VN: VU#800113
http://www.kb.cert.org/vuls/id/800113
* SECTRACK: 1020438
http://www.securitytracker.com/id?1020438
* SECTRACK: 1020440
http://www.securitytracker.com/id?1020440
* XF: win-dns-client-server-spoofing(43334)
http://xforce.iss.net/xforce/xfdb/43334

CVE Reference:

CVE-2008-1447 (cve.mitre.org, nvd.nist.gov)

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