ScoutNews
The weekly Security update from the makers of SecureScout
November 20, 2009

2009 Issue #47

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).

Download Here:
http://www.netvigilance.com/productdownloads?productname=messengerservicevulnerabilityscanner

This Week in Review

MAC & PC users equally exposed. Hacks of Kindness plan for disaster relief. Gov most worried about unstructured data. Law firms be aware of phishing attacks.

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

- **Survey finds Mac, PC users are equal cybercrime victims**

Mac enthusiasts are just as likely to fall victim to a phishing attack as Windows users, according to a survey commissioned by security firm ESET.

The survey of 1,003 people, conducted by Competitive Edge Research and Communications, concluded that most cybercrime losses are caused by phishing attacks, but that users are equally at risk to these ploys, no matter what operating system they leverage.

"Phishing attacks are just as effective on Macs, Linux, Windows, Solaris and any operating system since they rely on tricking the user and not on malicious software or any software vulnerabilities," Randy Abrams, director of technical education at ESET, said Monday in a blog post. "The Mac offers no immunity to phishing attacks and so we see a virtually equal percentage of victim representation across the board." SC Magazine

Full Story :
http://www.scmagazineus.com/survey-finds-mac-pc-users-are-equal-cybercrime-victims/article/157939/?utm_source

- **Audio Slideshow: Hackers use tech to solve disaster relief challenges**

Last week at the Hacker Dojo in Mountain View, Calif., developers partnered with Google, Yahoo, NASA, and the World Bank to exchange ideas and work on solutions for responding to natural disasters and other emergencies.

Random Hacks of Kindness is the first in a series of planned events that seek to use technology to solve real world problems related to crisis and disaster relief. By first working with governments and non-governmental organizations to better understand the immediate needs of rescuers and communities following a critical emergency, these programmers are work directly to solve communication issues and to better facilitate the exchange of information and resources in times of need.

Often, information comes from a wide array of sources during emergencies, including governments, rescuers, and victims in local communities. Successfully organizing the incoming content and delivering information back to the proper resource is a critical part of providing aid to victims. Cnet Security

Full Story :
http://news.cnet.com/8301-30252_3-10399130-246.html?part=rss&subj=news&tag=2547-1_3-0-20

- **Gov't executives cite unstructured data as top concern**

More than cloud computing, mobile devices and Web 2.0 applications, unstructured data is the cyberthreat federal government IT executives are most worried about, according to a survey released Wednesday by the Ponemon Institute and IT management software and solutions vendor CA.

In the survey of 217 senior IT executives from U.S. federal organizations, 79 percent said unstructured data - information not contained in databases - increases their organization's security risk. Unstructured data includes email and Word documents.

The common use of collaboration tools, such as SharePoint, also has caused an increase in the amount of stored unstructured data, which may contain confidential or sensitive information that is not always adequately safeguarded, Tim Brown, vice president and chief architect for security management at CA, told SCMagazineUS.com on Wednesday. SC Magazine

Full Story :
http://www.scmagazineus.com/govt-executives-cite-unstructured-data-as-top-concern/article/158049/?utm_source=f

- **Law, PR firms targeted**

The FBI warned Tuesday of an increase in targeted phishing emails containing malicious attachments or links that are being sent to law and public relations firms. If executed, the malicious payload used in the attack attempts to download and execute the file â€˜srhost.exe' from the domain â€˜http://d.ueopen.com,' the agency said in an alert. Any network traffic associated with the domain â€˜ueopen.com' should indicate a network is compromised. SC Magazine

Full Story :
http://www.scmagazineus.com/law-pr-firms-targeted/article/157967/?utm_source=feedburner&utm_medium=feed&ut

New Vulnerabilities Tested in SecureScout

- **13733 Oracle Database Server - Authentication component unspecified Vulnerability (oct-2009/CVE-2009-2000)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Authentication" component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html
* CERT: TA09-294A
http://www.us-cert.gov/cas/techalerts/TA09-294A.html
* BID: 36756
http://www.securityfocus.com/bid/36756
* SECTRACK: 1023057
http://www.securitytracker.com/id?1023057
* SECUNIA: 37027
http://secunia.com/advisories/37027

CVE Reference:

CVE-2009-2000 (cve.mitre.org, nvd.nist.gov)

• 13734 Oracle Database Server - Advanced Queuing component unspecified Vulnerability (oct-2009/CVE-2009-1995)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Advanced Queuing" component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html
* CERT: TA09-294A
http://www.us-cert.gov/cas/techalerts/TA09-294A.html
* BID: 36752
http://www.securityfocus.com/bid/36752
* OSVDB: 59109
http://osvdb.org/59109
* SECTRACK: 1023057
http://www.securitytracker.com/id?1023057
* SECUNIA: 37027
http://secunia.com/advisories/37027

CVE Reference:

CVE-2009-1995 (cve.mitre.org, nvd.nist.gov)

• 13735 Oracle Database Server - Oracle Text component unspecified Vulnerability (oct-2009/CVE-2009-1991)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Oracle Text" component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html
* CERT: TA09-294A
http://www.us-cert.gov/cas/techalerts/TA09-294A.html
* BID: 36748
http://www.securityfocus.com/bid/36748
* OSVDB: 59113
http://osvdb.org/59113
* SECTRACK: 1023057
http://www.securitytracker.com/id?1023057
* SECUNIA: 37027
http://secunia.com/advisories/37027

CVE Reference:

CVE-2009-1991 (cve.mitre.org, nvd.nist.gov)

• 13736 Oracle Database Server - Data Pump component unspecified Vulnerability (oct-2009/CVE-2009-1971)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Data Pump" component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html
* CERT: TA09-294A
http://www.us-cert.gov/cas/techalerts/TA09-294A.html
* BID: 36754
http://www.securityfocus.com/bid/36754
* SECTRACK: 1023057
http://www.securitytracker.com/id?1023057
* SECUNIA: 37027
http://secunia.com/advisories/37027

CVE Reference:

CVE-2009-1971 (cve.mitre.org, nvd.nist.gov)

• 13737 Oracle Database Server - Auditing component unspecified Vulnerability (oct-2009/CVE-2009-1972)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Auditing" component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html
* CERT: TA09-294A
http://www.us-cert.gov/cas/techalerts/TA09-294A.html
* BID: 36758
http://www.securityfocus.com/bid/36758
* SECTRACK: 1023057
http://www.securitytracker.com/id?1023057
* SECUNIA: 37027
http://secunia.com/advisories/37027

CVE Reference:

CVE-2009-1972 (cve.mitre.org, nvd.nist.gov)

• 18599 Web Services on Devices API Memory Corruption Vulnerability (MS09-063/973565) (Remote File Checking)

A remote code execution vulnerability exists in the Web Services on Devices API (WSDAPI) on Windows systems. The vulnerability is due to the service not properly handling a WSDAPI message with a specially crafted header. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

References:

* BID: 36919
http://www.securityfocus.com/bid/36919
* VUPEN: VUPEN/ADV-2009-3189
http://www.vupen.com/english/advisories/2009/3189
* SECTRACK: 1023153
http://securitytracker.com/alerts/2009/Nov/1023153.html
* MS: MS09-063
http://www.microsoft.com/technet/security/Bulletin/MS09-063.mspx
* CERT: TA09-314A
http://www.us-cert.gov/cas/techalerts/TA09-314A.html

CVE Reference:

CVE-2009-2512 (cve.mitre.org, nvd.nist.gov)

• 18600 License Logging Server Heap Overflow Vulnerability (MS09-064/974783) (Remote File Checking)

An unauthenticated remote code execution vulnerability exists in the way that the Microsoft License Logging Server software handles specially crafted RPC packets. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted network message to a computer running the License Logging service. An attacker who successfully exploited this vulnerability could take complete control of the system.

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

References:

* BID: 36921
http://www.securityfocus.com/bid/36921
* VUPEN: VUPEN/ADV-2009-3190
http://www.vupen.com/english/advisories/2009/3190
* SECTRACK: 1023154
http://securitytracker.com/alerts/2009/Nov/1023154.html
* MS: MS09-064
http://www.microsoft.com/technet/security/Bulletin/MS09-064.mspx
* CERT: TA09-314A
http://www.us-cert.gov/cas/techalerts/TA09-314A.html

CVE Reference:

CVE-2009-2523 (cve.mitre.org, nvd.nist.gov)

• 18601 LSASS Recursive Stack Overflow Vulnerability (MS09-066/973309) (Remote File Checking)

A denial of service vulnerability exists in implementations of Active Directory on Microsoft Windows 2000 Server, Windows Server 2003, and Windows Server 2008. The vulnerability also exists in implementations of Active Directory Application Mode (ADAM) when installed on Windows XP and Windows Server 2003, and Active Directory Lightweight Directory Service (AD LDS) on Windows Server 2008. The vulnerability is due to stack space exhaustion during execution of certain types of LDAP or LDAPS requests. An attacker who successfully exploited this vulnerability could cause the affected system to stop responding.

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

References:

* BID: 36918
http://www.securityfocus.com/bid/36918
* VUPEN: VUPEN/ADV-2009-3192
http://www.vupen.com/english/advisories/2009/3192
* SECTRACK: 1023156
http://securitytracker.com/alerts/2009/Nov/1023156.html
* MS: MS09-066
http://www.microsoft.com/technet/security/Bulletin/MS09-066.mspx
* CERT: TA09-314A
http://www.us-cert.gov/cas/techalerts/TA09-314A.html

CVE Reference:

CVE-2009-1928 (cve.mitre.org, nvd.nist.gov)

• 18602 Microsoft Office Word File Information Memory Corruption Vulnerability (MS09-068/976307) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Word handles a specially crafted Word file that includes a malformed record. 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:

* IDEFENSE: 20091110 Microsoft Word FIB Processing Stack Buffer Overflow Vulnerability
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=831
* MS: MS09-068
http://www.microsoft.com/technet/security/Bulletin/MS09-068.mspx
* CERT: TA09-314A
http://www.us-cert.gov/cas/techalerts/TA09-314A.html
* BID: 36950
http://www.securityfocus.com/bid/36950
* OSVDB: 59857
http://osvdb.org/59857
* SECTRACK: 1023158
http://www.securitytracker.com/id?1023158
* SECUNIA: 37277
http://secunia.com/advisories/37277
* VUPEN: ADV-2009-3194
http://www.vupen.com/english/advisories/2009/3194

CVE Reference:

CVE-2009-3135 (cve.mitre.org, nvd.nist.gov)

• 18603 Oracle Application Server - Business Intelligence Enterprise Edition component unspecified Vulnerability (oct-2009/CVE-2009-1999)

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Business Intelligence Enterprise Edition" component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html
* CERT: TA09-294A
http://www.us-cert.gov/cas/techalerts/TA09-294A.html
* BID: 36746
http://www.securityfocus.com/bid/36746
* OSVDB: 59118
http://osvdb.org/59118
* SECTRACK: 1023058
http://www.securitytracker.com/id?1023058
* SECUNIA: 37099
http://secunia.com/advisories/37099

CVE Reference:

CVE-2009-1999 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-3943 Microsoft CVSS 2.0 Score = 5.0

Microsoft Internet Explorer 6 through 6.0.2900.2180 and 7 through 7.0.6000.16711 allows remote attackers to cause a denial of service (application hang) via a JavaScript loop that configures the home page by using the setHomePage method and a DHTML behavior property.

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

References:

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/507760/100/0/threaded

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/507731/100/0/threaded

MISC: http://websecurity.com.ua/3658/

CVE Reference: CVE-2009-3943

• CVE-2009-3841 HP CVSS 2.0 Score = 9.0

Unspecified vulnerability in HP Discovery & Dependency Mapping Inventory (DDMI) 2.5x, 7.5x, and 7.60 on Windows allows remote authenticated users to execute arbitrary code via unknown vectors.

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

References:

SECTRACK: http://securitytracker.com/id?1023187

SECUNIA: http://secunia.com/advisories/37388

HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01861595

HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01861595

CVE Reference: CVE-2009-3841

• CVE-2009-3840 HP CVSS 2.0 Score = 5.0

The embedded database engine service (aka ovdbrun.exe) in HP OpenView Network Node Manager (OV NNM) 7.51 and 7.53 allows remote attackers to cause a denial of service (daemon crash) via an invalid Error Code field in a packet.

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

References:

BID: http://www.securityfocus.com/bid/37046

HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01926980

HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01926980

MISC: http://www.coresecurity.com/content/openview_nnm_internaldb_dos

FULLDISC: http://seclists.org/fulldisclosure/2009/Nov/199

CVE Reference: CVE-2009-3840

- **CVE-2009-3977 HP CVSS 2.0 Score = 5.0**

Multiple buffer overflows in a certain ActiveX control in ActiveDom.ocx in HP OpenView Network Node Manager (OV NNM) 7.53 might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via a long string argument to the (1) DisplayName, (2) AddGroup, (3) InstallComponent, or (4) Subscribe method. NOTE: this issue is not a vulnerability in many environments, because the control is not marked as safe for scripting and would not execute with default Internet Explorer settings.

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

References:

MISC: http://www.coresecurity.com/content/openview_nnm_internaldb_dos

FULLDISC: http://seclists.org/fulldisclosure/2009/Nov/199

CVE Reference: CVE-2009-3977

- **CVE-2009-2746 IBM CVSS 2.0 Score = 6.8**

Cross-site request forgery (CSRF) vulnerability in the administrative console in the Security component in IBM WebSphere Application Server (WAS) 6.0.2 before 6.0.2.39, 6.1 before 6.1.0.29, and 7.0 before 7.0.0.7 allows remote attackers to hijack the authentication of administrators via unspecified vectors.

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

References:

CONFIRM: http://www-01.ibm.com/support/docview.wss?uid=swg27014463

XF: http://xforce.iss.net/xforce/xfdb/54227

AIXAPAR: http://www-01.ibm.com/support/docview.wss?uid=swg1PK99477

AIXAPAR: http://www-01.ibm.com/support/docview.wss?uid=swg1PK87176

SECUNIA: http://secunia.com/advisories/37221

CVE Reference: CVE-2009-2746

- **CVE-2009-3889 Linux CVSS 2.0 Score = 6.6**

The dbg_lvl file for the megaraid_sas driver in the Linux kernel before 2.6.27 has world-writable permissions, which allows local users to change the (1) behavior and (2) logging level of the driver by modifying this file.

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

References:

MISC: https://bugzilla.redhat.com/show_bug.cgi?id=526068

MLIST: http://www.openwall.com/lists/oss-security/2009/11/13/4

MLIST: http://www.openwall.com/lists/oss-security/2009/11/13/1

CONFIRM: http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.27

CONFIRM: http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=66dca9b8c50b5e59d3bea8b21cee5c6dae6c9c46

CVE Reference: CVE-2009-3889

- **CVE-2009-3939 Linux CVSS 2.0 Score = 6.6**

The poll_mode_io file for the megaraid_sas driver in the Linux kernel 2.6.31.6 and earlier has world-writable permissions, which allows local users to change the I/O mode of the driver by modifying this file.

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

References:

MISC: https://bugzilla.redhat.com/show_bug.cgi?id=526068

MLIST: http://www.openwall.com/lists/oss-security/2009/11/13/1

CVE Reference: CVE-2009-3939

- **CVE-2009-3888 Linux CVSS 2.0 Score = 4.9**

The do_mmap_pgoff function in mm/nommu.c in the Linux kernel before 2.6.31.6, when the CPU lacks a memory management unit, allows local users to cause a denial of service (OOPS) via an application that attempts to allocate a large amount of memory.

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

References:

MLIST: http://www.openwall.com/lists/oss-security/2009/11/13/3

MLIST: http://www.openwall.com/lists/oss-security/2009/11/09/2

CONFIRM: http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.31.6

CONFIRM: http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=89a8640279f8bb78aaf778d1fc5c4a6778f18064

CVE Reference: CVE-2009-3888

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