netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 50

December 15, 2006

Table of Contents

Product Focus

Messenger Service Vulnerability Scanner – The 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

Targeted attacks rising. UK phishing rising extremely. Data security and outsourcing. Cybercrime economy.

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

- **Targeted security attacks on the rise**

Corporate and industrial espionage attacks are on the rise using targeted trojans intended to steal intellectual property and confidential information, according to the 2006 Annual MessageLabs Intelligence Report.

MessageLabs now intercepts two attacks each day, compared to one per week at the same point in 2005.

The targeted approach is prevalent in phishing attacks too, an increasingly dominant

force in all malicious emails intercepted by MessageLabs, with levels rising from 10.6 per cent in January to 68.8 per cent in December.

Computing

Full Story :
http://www.computing.co.uk/computing/news/2171089/targeted-attacks-rise

❖ UK phishing up 8000% in two years, says FSA

Government report shows massive rise in scams.

A report presented to the UK government by the Financial Services Authority (FSA), the UK's financial watchdog organisation, indicates that phishing incidents have increased by an enormous 8000% in the last two years.

The figures reveal a total of over £23 million raked in by scammers in the first half of 2006, with a similar haul expected for the rest of the year. Just 312 phishing incidents were recorded in the first half of 2005, compared with over 5,000 in the first six months of 2006.

While some commentators have mentioned the impact of improved detection and reporting on the figures, there is little doubt that increasing amounts of spam carrying phishing attempts, and increasing sophistication in the design and execution of phishing, are tricking personal details, and thus money, out of more and more people.

Virus bulletin

Full Story :
http://www.virusbtn.com/news/spam_news/2006/12_15.xml?rss=

❖ Data security top priority in BPO

Data security is seen as more important than employment laws in business process outsourcing (BPO) deals, a survey has found.

Ninety per cent of managers consider issues such as the protection of intellectual property rights, contract enforcement and data protection more relevant to their business than laws relating to the transfer of staff, according to new research from the National Outsourcing Association (NOA).

The top legal issues managers cited as important include the ability to enforce contracts with offshore providers (93 per cent), data protection that allows cross-border transfers (93 per cent) and technology transfer laws (83 per cent).

Nigel Roxburgh, research director at NOA, said the increased publicity surrounding data security in offshoring, such as Channel 4's recent Dispatches programme revealing data theft in Indian call centres, has played a role in raising concerns.

Silicon.com

Full Story :

http://services.silicon.com/bpo/0,3800004865,39164697,00.htm

- **Cybercrime set to develop its own economy**

Organised criminals will join forces with the hacker community to form a more organised cybercrime economy, predicts vendor Websense.

Criminals will buy, sell and trade hot commodities such as ready made cyber-attack toolkits and exploits to carry out zero-day vulnerabilities.

Websense experts also predict that Web 2.0 security issues will escalate as these technologies are rolled out in mass with security as an afterthought.

Dan Hubbard, vice president of security research, Websense, said:'Organised criminals are realising that the internet has been a largely untapped resource in terms of generating real profit—until now. With financial gain on the table, attack methods are improving, and the number of people involved is escalating.'

vnunet

Full Story :
http://www.vnunet.com/computing/news/2171083/websense-predictions

New Vulnerabilities Tested in SecureScout

- **13503 Oracle Database Server - Environment Variable Vulnerabilities (Alert 23/apr-02)**

When the ORACLE_HOME environment variable contains 750 bytes or more, a buffer overflow occurs. This buffer overflow may potentially be used to overwrite variables on an application/OS memory stack. Since the dbsnmp program runs as SETUID root, it is possible to gain elevated privileges, including administrative access, on the operating system (OS). To exploit this vulnerability, the "oracle" user must belong to the "dba" OS group (OSDBA).

The "dbsnmp" executable executes the CHOWN and CHGRP commands on Unix (and Linux) platforms when it runs without using a statically declared path or without first checking the validity of the PATH environment variable specified by the user. Thus, a local user can
potentially gain elevated privileges, including root access, on the host operating system.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/dbsnmp_alert.pdf

Other references:
N.A.

Product Homepage:
http://www.oracle.com/

CVE Reference:

❖ 13504 Oracle Database Server - Buffer Overflow Vulnerability in the Oracle8i Listener (Alert 15/apr-02)

A potential security vulnerability has been discovered in the Oracle8i database server listener.

This vulnerability may cause a buffer overflow condition that allows remote execution of arbitrary code on the database server under a security context that grants full control of the database services and, on some platforms, full control of the operating system.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/nai_net8_bof.pdf

Other references:
N.A.

Product Homepage:
http://www.oracle.com/

CVE Reference:

❖ 13505 Oracle Database Server - Oracle Net8 Denial of Service Vulnerabilities (Alert 14)

1. Offset_to_data value too large:

A potential security vulnerability has been discovered in Net8 (formerly known as SQL*Net).
When connecting to an Oracle database, a connection is first made to the listener process. This initial packet contains command data, such as the instance to connect to and the client information. This packet also contains a header with a field indicating the offset to the Oracle command data. If this offset is set to an arbitrarily large value that the listener does not expect, then the listener will crash.

2. Requester_version value incorrect:

A potential security vulnerability has been discovered in Net8 (formerly known as SQL*Net).
When connecting to an Oracle database, a connection is first made to the listener process. This initial packet contains command data, such as the instance to connect to and the client information. This packet also contains a header with a field

indicating the version of the client drivers and the offset to the Oracle command data. If the version of the driver does not match to the appropriate offset to the command data, the listener will crash.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/net8_dos_alert.pdf

Other references:
N.A.

Product Homepage:
http://www.oracle.com/

CVE Reference:

❖ 13506 Oracle Database Server - Oracle Net8 Denial of Service Vulnerability (Alert 13)

A potential security vulnerability has been identified in redirected Net8 connections to the Oracle database server. This vulnerability allows an unauthenticated user to consume all the operating system memory on an Oracle server, remote users to deny access to all other users and cause the operating system to crash: Access to the server is denied and a reboot of the server is required.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/net8_dos_redirect_alert.pdf

Other references:
N.A.

Product Homepage:
http://www.oracle.com/

CVE Reference:

❖ 13507 Oracle Database Server - Oracle Connection Manager Control SUID Vulnerability

A potential security vulnerability has been discovered in Oracle Connection Manager Control (CMCTL). This vulnerability can force a buffer overflow in CMCTL which can be exploited to gain elevated operating system privilege sets of EGID DBA

and EUID ORACLE by an ordinary
user supplying command-line arguments to CMCTL. This vulnerability is only possible if SETGID and SETUID bits, respectively, are set on the CMCTL executable.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cmctl_alert.pdf

Other references:
N.A.

Product Homepage:
http://www.oracle.com/

CVE Reference:

❖ 16366 Cumulative Security Update for Internet Explorer (MS06-072/925454) (Remote File Checking)

A remote code execution vulnerability exists in Internet Explorer due to attempts to access previously freed memory when handling script errors in certain situations. An attacker could exploit the vulnerability by constructing a specially crafted Web page. If a user viewed the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

A remote code execution vulnerability exists in the way Internet Explorer interprets certain DHTML script function calls to incorrectly created elements. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code execution if a user viewed the Web page. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

An information disclosure vulnerability exists in Internet Explorer in the way that drag and drop operations are handled in certain situations. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could allow for information disclosure if a user viewed and interacted with the Web page. An attacker who successfully exploited this vulnerability would be able to retrieve files from the Temporary Internet Files (TIF) folder on a user's system.

An information disclosure vulnerability exists in Internet Explorer in certain scenarios where the path to the cached content in the TIF folder could be disclosed. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could allow for information disclosure if a user viewed the Web page. An attacker who successfully exploited this vulnerability would be able to retrieve files from the Temporary Internet Files (TIF) folder on a user's system. However, user interaction is required to exploit this vulnerability.

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

References:

Original advisory:
MS06-072
http://www.microsoft.com/technet/security/bulletin/ms06-072.mspx

Other references:
* MISC: http://www.zerodayinitiative.com/advisories/ZDI-06-048.html

CVE Reference: CVE-2006-5579
CVE-2006-5581
CVE-2006-5578
CVE-2006-5577

❖ 16367 Vulnerability in Visual Studio 2005 Could Allow Remote Code Execution (MS06-073/925674) (Remote File Checking)

A remote code execution vulnerability exists in the WMI Object Broker control that the WMI Wizard uses in Visual Studio 2005. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code execution if a user viewed the Web page. 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:

Original advisory:
MS06-073
http://www.microsoft.com/technet/security/bulletin/ms06-073.mspx

Other references:
MISC: http://research.eeye.com/html/alerts/zeroday/20061031.html
MISC: http://www.zerodayinitiative.com/advisories/ZDI-06-047.html
CONFIRM: http://blogs.technet.com/msrc/archive/2006/11/01/microsoft-security-advisory-927709-posted.aspx
MSKB:927709
URL:http://www.microsoft.com/technet/security/advisory/927709.mspx
CERT-VN:VU#854856
URL:http://www.kb.cert.org/vuls/id/854856
BID:20843
URL:http://www.securityfocus.com/bid/20843
FRSIRT:ADV-2006-4282
URL:http://www.frsirt.com/english/advisories/2006/4282
SECTRACK:1017142
URL:http://securitytracker.com/id?1017142
SECUNIA:22603
URL:http://secunia.com/advisories/22603

CVE Reference: CVE-2006-4704

❖ 16368 Vulnerability in SNMP Could Allow Remote Code Execution

(MS06-074/926247) (Remote File Checking)

A remote code execution vulnerability exists in SNMP Service that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

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

References:

Original advisory:
MS06-074
http://www.microsoft.com/technet/security/bulletin/ms06-074.mspx

Other references:
http://secunia.com/cve_reference/CVE-2006-5583/
http://www.securiteam.com/windowsntfocus/6J00D0UHPM.html

CVE Reference: CVE-2006-5583

❖ **16369 Vulnerability in Windows Could Allow Elevation of Privilege (MS06-075/926255) (Remote File Checking)**

A privilege elevation vulnerability exists in the way that Microsoft Windows starts applications with specially crafted file manifests. This vulnerability could allow a logged on user to take complete control of the system.

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

References:

Original advisory:
MS06-075
http://www.microsoft.com/technet/security/Bulletin/MS06-075.mspx

Other references:
SECUNIA:23308
URL:http://secunia.com/advisories/23308

CVE Reference: CVE-2006-5585

❖ **16370 Cumulative Security Update for Outlook Express (MS06-076/923694) (Remote File Checking)**

A remote code execution vulnerability in a component of Outlook Express could allow an attacker who sent a Windows Address Book file to a user of an affected system to take complete control of the system.

If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new

accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

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

References:

Original advisory:
MS06-076
http://www.microsoft.com/technet/security/Bulletin/MS06-076.mspx

Other references:
http://secunia.com/cve_reference/CVE-2006-2386/
http://www.frsirt.com/english/CVE-2006-2386.php

CVE Reference: CVE-2006-2386

New Vulnerabilities found this Week

OpenLDAP "krbv4_ldap_auth()" Buffer Overflow Vulnerability

"Execution of arbitrary code"

Solar Eclipse has reported a vulnerability in OpenLDAP, which can be exploited by malicious people to potentially compromise a vulnerable system.

The vulnerability is caused due to a boundary error within the "krbv4_ldap_auth()" function in servers/slapd/kerberos.c and can be exploited to cause a stack based buffer overflow by sending a specially crafted bind request with more than 1250 bytes of credential data.

Successful exploitation may allow the execution of arbitrary code, but requires that OpenLDAP is compiled with the "--enable-kbind" option (not enabled by default since version 2.0.2 and removed from the configure script since version 2.1).

References:
http://www.phreedom.org/solar/exploits/openldap-kbind/

Clam AntiVirus Multipart Nestings Denial of Service

"Denial of Service"

Hendrik Weimer has reported a vulnerability in Clam AntiVirus, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to a stack overflow when scanning messages with deeply nested multipart content. This can be exploited to crash the service by sending specially crafted emails to a vulnerable system.

The vulnerability is reported in versions prior to 0.88.7.

References:
http://www.quantenblog.net/security/virus-scanner-bypass

Windows Remote Installation Service Writable Path Vulnerability
"Upload malicious files; overwrite existing operating system files"

A vulnerability has been reported in Microsoft Windows, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to the Remote Installation Service enabling a TFTP service, which by default allows anonymous users to upload malicious files or overwrite existing operating system files.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-077.mspx

Outlook Express Address Book Contact Record Vulnerability
"Execution of arbitrary code"
A vulnerability has been reported in Outlook Express, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error within the processing of Windows Address Book files (.wab) and can be exploited to cause a buffer overflow by tricking a user into opening a specially crafted WAB file.

Successful exploitation allows execution of arbitrary code.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-076.mspx
http://descriptions.securescout.com/tc/16370

Microsoft Windows File Manifest Privilege Escalation Vulnerability
"Gain escalated privileges"

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

The vulnerability is caused due to an error in the Client-Server Run-time Subsystem when processing file manifests and can be exploited by starting up an applications with specially crafted file manifest.

Successful exploitation allows execution of arbitrary code with escalated privileges.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-075.mspx

Microsoft Windows SNMP Service Buffer Overflow Vulnerability
"Execution of arbitrary code"

A vulnerability has been reported in Microsoft Windows, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the SNMP service and can be exploited to cause a buffer overflow via a specially crafted message.

Successful exploitation allows execution of arbitrary code.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-074.mspx
http://descriptions.securescout.com/tc/16368

Internet Explorer Multiple Vulnerabilities
"Execute arbitrary code; retrieve content of the TIF folder"

Some vulnerabilities have been reported in Internet Explorer, which can be exploited by malicious people to gain knowledge of certain information or potentially compromise a user's system.

1) A memory corruption error within the interpretation of certain DHTML script function calls (e.g. normalize()) to incorrectly created elements can potentially be exploited to execute arbitrary code on a user's system.

2) An unspecified error within the handling of drag and drop operations can be exploited to retrieve content of the TIF folder (Temporary Internet Files) via a specially crafted web page.

3) An unspecified error within the handling of OBJECT tags can be exploited to disclose the path to the TIF folder (Temporary Internet Files) and retrieve its contents via a specially crafted web page.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-072.mspx
http://descriptions.securescout.com/tc/16366

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