netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 43

November 2, 2007

Table of Contents

Product Focus

netVigilance has migrated SecureScout to CVSS 2.0 (Common Vulnerability Scoring System) for all test cases.
CVSS 2.0's metric system reflects the severity of vulnerabilities better than CVSS 1.0.
The CVSS base score is a cornerstone in calculating the asset risk exposure of the new asset value feature of SecureScout SP.

This week netVigilance Security Research has found 3 vulnerabilities in open source software Saxon:
1 medium risk with CVSS 2.0 base score 5 and 2 high risk with CVSS 2.0 base scores 7.5 and 8.3. 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

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

Jesper Jurcenoks, CTO for NetVigilance, in experts panel during the Chicago ITEC. Still no ruling on domain owner privacy. VoIP may be next big spam target. Security panel to craft US security standards.

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

❖ Vulnerability assessment

How to test every network device before hackers do.
Hackers attack systems by throwing their bag of tricks at a network device and sneaking in through any cracks they find. But they don't just attack computers any more; they're targeting anything with an IP address, such as routers, printers, network-attached storage units, wireless access points and backup appliances. Their motto is simple: have IP address, hack IP address.

Jesper Jurcenoks, CTO for NetVigilance, anchored the "Security 2008: What You Need Now" panel of experts during the Chicago ITEC conference.
His company specializes in vulnerability assessment, the practice of checking company networks for holes that hackers could use to attack your systems.

Network world

Full Story :
http://www.networkworld.com/columnists/2007/102907gaskin.html?fsrc=rss-columns

❖ ICANN Defers Ruling on Whois Privacy

"We seem to be closing off the development process at the same time we're opening the box to the same old debates that have been going on for seven years," complained Milton Mueller, a Syracuse University professor on the committee. "The whole world is watching now. ... They're expecting ICANN to do something about this."
A panel on Internet names voted Wednesday to defer long-simmering questions on whether names, phone numbers and other private information on domain name owners should remain public in open, searchable databases called Whois.

Cio today

Full Story :
http://www.cio-today.com/news/ICANN-Defers-Ruling-on-Whois-Privacy/story.xhtml?story_id=0010003B3WIW

❖ Why VoIP is the next target for spammers

Industry experts believe that attacks over services such as Skype are moving from proof of concept to becoming a real threat
In what looks like a highly developed piece of irony, hackers have proven that Voice over internet Telephony (VoIP) accounts are prone to the nuisance of voice spam - by attacking the university where the co-author of the protocol that VoIP runs on is professor of computer science.

Guardian unlimited

Full Story :
http://www.guardian.co.uk/technology/2007/nov/01/news.hacking?gusrc=rss&feed=technology

- **Task force aims to improve U.S. cybersecurity**

A blue-ribbon panel of three dozen security experts hopes to craft a strategy to improve the United States' cybersecurity by the time the next president takes office, the Center for Strategic and International Studies (CSIS), and the task force's Congressional sponsors, announced on Tuesday.
The bipartisan Commission on Cyber Security for the 44th Presidency will be tasked with creating a plan to secure the nation's computers and critical infrastructure and presenting that plan to the next president. The task force is headed by Representatives Jim Langevin (D-RI) and Michael McCaul (R-TX), Microsoft's vice president for Trustworthy Computing Scott Charney and retired Navy admiral Bobby Inman.

Security focus

Full Story :
http://www.securityfocus.com/news/11494?ref=rss

New Vulnerabilities Tested in SecureScout

- **13589 MySQL CREATE TABLE LIKE Information Disclosure Vulnerability**

MySQL Server does not require privileges such as SELECT for the source table in a CREATE TABLE LIKE statement, which allows remote authenticated users to obtain sensitive information such as the table structure.

The security issue has been reported in versions prior to 5.0.44 and 5.1.20.

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

References:

* BUGTRAQ: 20070717 rPSA-2007-0143-1 mysql mysql-bench mysql-server
http://www.securityfocus.com/archive/1/archive/1/473874/100/0/threaded
* MLIST: [announce] 20070712 MySQL Community Server 5.0.45 has been released!
http://lists.mysql.com/announce/470
* MISC:
http://bugs.mysql.com/bug.php?id=25578
* CONFIRM:
https://issues.rpath.com/browse/RPL-1536
* CONFIRM:
http://dev.mysql.com/doc/refman/5.0/en/releasenotes-cs-5-0-45.html
* GENTOO: GLSA-200708-10
http://security.gentoo.org/glsa/glsa-200708-10.xml
* REDHAT: RHSA-2007:0894
http://www.redhat.com/support/errata/RHSA-2007-0894.html

* BID: 25017
http://www.securityfocus.com/bid/25017
* SECUNIA: 26073
http://secunia.com/advisories/26073
* SECUNIA: 26498
http://secunia.com/advisories/26498
* SECUNIA: 25301
http://secunia.com/advisories/25301
* SECUNIA: 26987
http://secunia.com/advisories/26987
* SECUNIA: 26430
http://secunia.com/advisories/26430

CVE Reference: CVE-2007-3781

❖ 13588 MySQL malformed password packet Denial of Service Vulnerability

MySQL Server allows remote attackers to cause a denial of service (daemon crash) via a malformed password packet in the connection protocol.

The security issue has been reported in versions prior to 4.1.24, 5.0.44 and 5.1.20.

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

References:

* BUGTRAQ: 20070717 rPSA-2007-0143-1 mysql mysql-bench mysql-server
http://www.securityfocus.com/archive/1/archive/1/473874/100/0/threaded
* MLIST: [announce] 20070712 MySQL Community Server 5.0.45 has been released!
http://lists.mysql.com/announce/470
* MISC:
http://bugs.mysql.com/bug.php?id=28984
* CONFIRM:
https://issues.rpath.com/browse/RPL-1536
* CONFIRM:
http://dev.mysql.com/doc/refman/5.0/en/releasenotes-cs-5-0-45.html
* GENTOO: GLSA-200708-10
http://security.gentoo.org/glsa/glsa-200708-10.xml
* MANDRIVA: MDKSA-2007:177
http://www.mandriva.com/security/advisories?name=MDKSA-2007:177
* REDHAT: RHSA-2007:0894
http://www.redhat.com/support/errata/RHSA-2007-0894.html
* REDHAT: RHSA-2007:0875
http://www.redhat.com/support/errata/RHSA-2007-0875.html
* SUSE: SUSE-SR:2007:019
http://www.novell.com/linux/security/advisories/2007_19_sr.html
* UBUNTU: USN-528-1
http://www.ubuntulinux.org/support/documentation/usn/usn-528-1
* BID: 25017
http://www.securityfocus.com/bid/25017

* SECTRACK: 1018629
http://www.securitytracker.com/id?1018629
* SECUNIA: 26073
http://secunia.com/advisories/26073
* SECUNIA: 26498
http://secunia.com/advisories/26498
* SECUNIA: 26710
http://secunia.com/advisories/26710
* SECUNIA: 25301
http://secunia.com/advisories/25301
* SECUNIA: 26987
http://secunia.com/advisories/26987
* SECUNIA: 26621
http://secunia.com/advisories/26621
* SECUNIA: 27155
http://secunia.com/advisories/27155
* SECUNIA: 26430
http://secunia.com/advisories/26430

CVE Reference: CVE-2007-3780

❖ **13587 MySQL ALTER TABLE statement Information disclosure Vulnerability**

MySQL allows remote authenticated users without SELECT privileges to obtain sensitive information from partitioned tables via an ALTER TABLE statement.

The security issue has been reported in versions 5.1.x prior to 5.1.18.

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

References:

* MISC:
http://bugs.mysql.com/bug.php?id=23675
* CONFIRM:
http://dev.mysql.com/doc/refman/5.1/en/news-5-1-18.html
* BID: 24008
http://www.securityfocus.com/bid/24008
* FRSIRT: ADV-2007-1804
http://www.frsirt.com/english/advisories/2007/1804
* SECTRACK: 1018071
http://www.securitytracker.com/id?1018071
* SECUNIA: 25301
http://secunia.com/advisories/25301

CVE Reference: CVE-2007-2693

❖ 13586 Oracle Database Server - Spatial component unspecified Vulnerability (oct-2007/DB27)

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

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html
* CERT: TA07-290A
http://www.us-cert.gov/cas/techalerts/TA07-290A.html
* FRSIRT: ADV-2007-3524
http://www.frsirt.com/english/advisories/2007/3524
* SECTRACK: 1018823
http://www.securitytracker.com/id?1018823
* SECUNIA: 27251
http://secunia.com/advisories/27251

CVE Reference: CVE-2007-5515

❖ 13585 Oracle Database Server - SQL Execution component unspecified Vulnerability (oct-2007/DB26)

An unspecified vulnerability with unknown impact exists in Oracle Database Server SQL Execution component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html
* CERT: TA07-290A
http://www.us-cert.gov/cas/techalerts/TA07-290A.html
* FRSIRT: ADV-2007-3524
http://www.frsirt.com/english/advisories/2007/3524
* SECTRACK: 1018823
http://www.securitytracker.com/id?1018823
* SECUNIA: 27251
http://secunia.com/advisories/27251

CVE Reference: CVE-2007-5514

❖ 13584 Oracle Database Server - Advanced Queuing component

unspecified Vulnerability (oct-2007/DB25)

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/cpuoct2007.html
* CERT: TA07-290A
http://www.us-cert.gov/cas/techalerts/TA07-290A.html
* FRSIRT: ADV-2007-3524
http://www.frsirt.com/english/advisories/2007/3524
* SECTRACK: 1018823
http://www.securitytracker.com/id?1018823
* SECUNIA: 27251
http://secunia.com/advisories/27251

CVE Reference: CVE-2007-5504

❖ **13583 Oracle Database Server - Oracle Database Vault component unspecified Vulnerability (oct-2007/DB24)**

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

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html
* CERT: TA07-290A
http://www.us-cert.gov/cas/techalerts/TA07-290A.html
* FRSIRT: ADV-2007-3524
http://www.frsirt.com/english/advisories/2007/3524
* SECTRACK: 1018823
http://www.securitytracker.com/id?1018823
* SECUNIA: 27251
http://secunia.com/advisories/27251

CVE Reference: CVE-2007-5514

❖ **13582 Oracle Database Server - XML DB component unspecified Vulnerability (oct-2007/DB23)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server XML DB component.

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

References:

* BUGTRAQ: 20071017 Oracle audit issue with XMLDB ftp service
http://www.securityfocus.com/archive/1/archive/1/482426/100/0/threaded
* MISC:
http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-oracle-xmldb-ftp-service/
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html
* CERT: TA07-290A
http://www.us-cert.gov/cas/techalerts/TA07-290A.html
* BID: 26107
http://www.securityfocus.com/bid/26107
* FRSIRT: ADV-2007-3524
http://www.frsirt.com/english/advisories/2007/3524
* SECTRACK: 1018823
http://www.securitytracker.com/id?1018823
* SECUNIA: 27251
http://secunia.com/advisories/27251

CVE Reference: CVE-2007-5513

❖ 13581 Oracle Database Server - Oracle Net Services component unspecified Vulnerability (oct-2007/DB22)

An unspecified vulnerability with unknown impact exists in Oracle Database Server Oracle Net Services component.

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

References:

* BUGTRAQ: 20071017 Oracle TNS Listener DoS and/or remote memory inspection
http://www.securityfocus.com/archive/1/archive/1/482423/100/0/threaded
* MISC:
http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-oracle-tns-listener/
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html
* CERT: TA07-290A
http://www.us-cert.gov/cas/techalerts/TA07-290A.html
* BID: 26103
http://www.securityfocus.com/bid/26103
* FRSIRT: ADV-2007-3524
http://www.frsirt.com/english/advisories/2007/3524
* SECTRACK: 1018823
http://www.securitytracker.com/id?1018823
* SECUNIA: 27251
http://secunia.com/advisories/27251

CVE Reference: CVE-2007-5507

❖ **13580 Oracle Database Server - Oracle Database Vault component unspecified Vulnerability (oct-2007/DB21)**

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

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html
* CERT: TA07-290A
http://www.us-cert.gov/cas/techalerts/TA07-290A.html
* FRSIRT: ADV-2007-3524
http://www.frsirt.com/english/advisories/2007/3524
* SECTRACK: 1018823
http://www.securitytracker.com/id?1018823
* SECUNIA: 27251
http://secunia.com/advisories/27251

CVE Reference: CVE-2007-5512

New Vulnerabilities found this Week

McAfee E-Business Server Authentication Packet Handling Buffer Overflow

"Execution of arbitrary code"

Secunia Research has discovered a vulnerability in McAfee E-Business Server, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an integer overflow within the e-Business administration utility service when parsing authentication packets. This can be exploited to cause a heap-based buffer overflow via a specially crafted authentication packet with an overly large length value.

Successful exploitation allows execution of arbitrary code.

References:
http://secunia.com/secunia_research/2007-69/

Symantec Mail Security for Exchange File Parsing Vulnerabilities

"Denial of Service; Execution of arbitrary code"

Multiple vulnerabilities have been discovered in Symantec Mail Security for Exchange, which can be exploited by malicious people to cause a DoS (Denial of Service) and compromise a vulnerable system.

The vulnerabilities are caused due to various errors within certain third-party file viewers and can be exploited to cause buffer overflows when a specially crafted file is checked.

Successful exploitation allows execution of arbitrary code, but requires that e.g. a policy is setup for scanning the contents of messages.

The vulnerabilities are confirmed in version 5.0.7.373. Other versions may also be affected.

References:
http://secunia.com/advisories/27304/

Novell BorderManager Client Trust Buffer Overflow Vulnerability
"Execution of arbitrary code"

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

The vulnerability is caused due to the Client Trust application incorrectly processing validation requests sent to the UDP port on which clntrust.exe is listening (by default 3024). This can be exploited to cause a heap-based buffer overflow by sending a specially crafted validation request containing a Novell tree name without backslash or zero wide characters.

Successful exploitation allows execution of arbitrary code.

The vulnerability is reported in Novell BorderManager 3.8. Prior versions may also be affected.

References:

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