netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 42

October 26, 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.

CodeRed Worm Scanner – The CodeRed Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any have been infected by CodeRed Worm.

This Week in Review

Ex-con on fraud at RSA.End Users show massive interest in IiPSEC 2008. Use of biometrics a hazard to privacy. ICAN onto insider information usage.

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

- **Security guru notes how IT eases committing fraud**

Frank Abagnale doesn't use online banking, thinks ID cards are a bad idea, and reckons the U.K. needs data breach notification laws.
Fraud expert, author and ex-con artist Frank Abagnale doesn't use online banking, thinks ID cards are a bad idea, and reckons the U.K. needs data breach notification laws.

"You can have the most sophisticated software in the world, the best technology. All it takes is one weak link in the chain," said Abagnale.

In a wide-ranging interview conducted as the closing keynote at the RSA Conference Europe event in London, Abagnale discussed how technology has made it easier than ever to commit fraud.

ARN

Full Story :
http://www.arnnet.com.au/index.php/id;1257038442;fp;16;fpid;1

❖ IIPSEC 2008 runs from January 29 to 31 at Stoneleigh Park, near Coventry.

With arrangements for IIPSEC 2008 well underway some trends are emerging, organisers report. The team behind IIPSEC are reporting that there has been a considerable swing towards End Users and consultants registering for the event now representing nearly half of the registrations (48pc), installer-integrators close behind with 38pc.

Event Director Kevin Fagan said: "The shift towards interest from end-users and consultants in-line with global market trends as IP is no longer a 'black art'. The major change this year is we are seeing more and more 'security and IT managers' register to attend as they are keen to see for themselves the benefits of the technology."

Professional Security

Full Story :
http://www.professionalsecurity.co.uk/newsdetails.aspx?NewsArticleID=7881&imgID=1

❖ Biometrics 2007: Biometrics help security trump privacy

Biometric technologies and plans for increased surveillance are jeopardising society's right to liberty and privacy, David Murakami Wood, managing editor of Surveillance & Society, said at the Biometrics 2007 conference last week.

Biometric technologies are increasingly emerging into society. They were initially used in airports but are now becoming commonplace in schools, bars and elsewhere, he said.

computerweekly

Full Story :
http://www.computerweekly.com/Articles/2007/10/30/227682/biometrics-2007-biometrics-help-security-trump-privacy.htm

❖ ICANN investigates domain name sharp practice

Internet oversight agency ICANN has launched an investigation into the possibility that insider information is being used to snap up desirable domain names before the person or organisation likely to be interested in them has had a chance to buy.

ICANN's Security and Stability Advisory Committee is looking into suspicions that someone with access to search requests has been using this data to snap up potentially desirable domains, a process dubbed domain name front running.

The Register

Full Story :
http://www.theregister.co.uk/2007/10/25/domain_name_front_running/

New Vulnerabilities Tested in SecureScout

❖ 13579 Oracle Database Server - Core RDBMS component unspecified Vulnerability (oct-2007/DB20)

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

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

References:

* BUGTRAQ: 20071017 Oracle RDBMS TNS Data packet DoS
http://www.securityfocus.com/archive/1/archive/1/482424/100/0/threaded
* 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-2007-5506

❖ 13578 Oracle Database Server - Advanced Security Option component unspecified Vulnerability (oct-2007/DB19)

An unspecified vulnerability with unknown impact exists in Oracle Database Server Advanced Security Option 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-2007-5505

❖ 13577 Oracle Database Server - Workspace Manager component unspecified Vulnerability (oct-2007/DB18)

An unspecified vulnerability with unknown impact exists in Oracle Database Server Workspace Manager 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
* BUGTRAQ: 20071017 SQL Injection Flaw in Oracle Workspace Manager
http://www.securityfocus.com/archive/1/archive/1/482429/100/0/threaded
* BID: 26098
http://www.securityfocus.com/bid/26098

CVE Reference: CVE-2007-5510

❖ 13576 Oracle Database Server - Workspace Manager component unspecified Vulnerability (oct-2007/DB17)

An unspecified vulnerability with unknown impact exists in Oracle Database Server Workspace Manager 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
* BUGTRAQ: 20071017 SQL Injection Flaw in Oracle Workspace Manager
http://www.securityfocus.com/archive/1/archive/1/482429/100/0/threaded
* BID: 26098
http://www.securityfocus.com/bid/26098

CVE Reference: CVE-2007-5510

❖ 13575 Oracle Database Server - Workspace Manager component unspecified Vulnerability (oct-2007/DB16)

An unspecified vulnerability with unknown impact exists in Oracle Database Server Workspace Manager 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
* BUGTRAQ: 20071017 SQL Injection Flaw in Oracle Workspace Manager
http://www.securityfocus.com/archive/1/archive/1/482429/100/0/threaded
* BID: 26098
http://www.securityfocus.com/bid/26098

CVE Reference: CVE-2007-5510

❖ 13574 Oracle Database Server - Workspace Manager component unspecified Vulnerability (oct-2007/DB15)

An unspecified vulnerability with unknown impact exists in Oracle Database Server Workspace Manager 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
* BUGTRAQ: 20071017 SQL Injection Flaw in Oracle Workspace Manager
http://www.securityfocus.com/archive/1/archive/1/482429/100/0/threaded
* BID: 26098
http://www.securityfocus.com/bid/26098

CVE Reference: CVE-2007-5510

❖ 13573 Oracle Database Server - Workspace Manager component unspecified Vulnerability (oct-2007/DB14)

An unspecified vulnerability with unknown impact exists in Oracle Database Server Workspace Manager 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

* BUGTRAQ: 20071017 SQL Injection Flaw in Oracle Workspace Manager
http://www.securityfocus.com/archive/1/archive/1/482429/100/0/threaded
* BID: 26098
http://www.securityfocus.com/bid/26098

CVE Reference: CVE-2007-5510

❖ 13572 Oracle Database Server - Workspace Manager component unspecified Vulnerability (oct-2007/DB13)

An unspecified vulnerability with unknown impact exists in Oracle Database Server Workspace Manager 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
* BUGTRAQ: 20071017 SQL Injection Flaw in Oracle Workspace Manager
http://www.securityfocus.com/archive/1/archive/1/482429/100/0/threaded
* BID: 26098
http://www.securityfocus.com/bid/26098

CVE Reference: CVE-2007-5510

❖ 13571 Oracle Database Server - Workspace Manager component unspecified Vulnerability (oct-2007/DB12)

An unspecified vulnerability with unknown impact exists in Oracle Database Server Workspace Manager 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
* BUGTRAQ: 20071017 SQL Injection Flaw in Oracle Workspace Manager
http://www.securityfocus.com/archive/1/archive/1/482429/100/0/threaded
* BID: 26098
http://www.securityfocus.com/bid/26098

CVE Reference: CVE-2007-5510

❖ 13570 Oracle Database Server - Workspace Manager component unspecified Vulnerability (oct-2007/DB11)

An unspecified vulnerability with unknown impact exists in Oracle Database Server Workspace Manager 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
* BUGTRAQ: 20071017 SQL Injection Flaw in Oracle Workspace Manager
http://www.securityfocus.com/archive/1/archive/1/482429/100/0/threaded
* BID: 26098
http://www.securityfocus.com/bid/26098

CVE Reference: CVE-2007-5510

New Vulnerabilities found this Week

RealPlayer Playlist Handling Buffer Overflow Vulnerability

"Execution of arbitrary code"

A vulnerability has been discovered in RealPlayer, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a signedness error in MPAMedia.dll when handling playlist names. This can be exploited to cause a stack-based buffer overflow by e.g.

importing a file into a specified playlist with an overly long name via the "Import()" method of the IERPCtl ActiveX control (ierpplug.dll).

Successful exploitation allows execution of arbitrary code.

References:
http://service.real.com/realplayer/security/191007_player/en/
http://docs.real.com/docs/security/SecurityUpdate101907Player.pdf
http://www.kb.cert.org/vuls/id/871673

IBM Lotus Notes Multiple Vulnerabilities

"Execution of arbitrary code; Information disclosure"

Multiple vulnerabilities have been reported in IBM Lotus Notes, which can be exploited by malicious, local users to gain knowledge of potentially sensitive information and by malicious people to bypass certain security mechanisms or compromise a user's system.

1) Errors within various third-party file viewers (mifsr.dll, awsr.dll, kpagrdr.dll, exesr.dll, rtfsr.dll, mwsr.dll, exesr.dll, wp6sr.dll, and lasr.dll) can be exploited to cause buffer overflows by tricking a user into viewing a specially crafted attachment.

Successful exploitation may allow execution of arbitrary code.

2) A boundary error when parsing HTML messages in nnotes.dll can be exploited to cause a buffer overflow when a user acts upon a malicious HTML message (e.g. replying, forwarding, or copying it to the clipboard).

Successful exploitation may allow execution of arbitrary code.

3) An error in the ECL (Execution Control List) mechanism may result in attachments being executed automatically instead of displaying the Execution Security Alert when handling Notes database (.nsf) and Notes template (.ntf) attachments.

4) Insecure permissions on shared memory allow any local user to access memory containing other users' data.

A bug was also reported, which may crash the client when receiving specially crafted SMTP responses.

References:
http://www-1.ibm.com/support/docview.wss?uid=swg21271111
http://www-1.ibm.com/support/docview.wss?uid=swg21272836
http://www-1.ibm.com/support/docview.wss?uid=swg21272930
http://www-1.ibm.com/support/docview.wss?uid=swg21270884
http://www-1.ibm.com/support/docview.wss?uid=swg21257030
http://www-1.ibm.com/support/docview.wss?uid=swg21271957

Apache Tomcat WebDAV Arbitrary File Content Disclosure

"Information disclosure"

eliteb0y has reported a vulnerability in Apache Tomcat, which can be exploited by malicious users to disclose potentially sensitive information.

The vulnerability is caused due to an error within the WebDAV servlet when configured for use with a context and enabled for write. This can be exploited to disclose the contents of arbitrary files via specially-crafted WebDAV requests that specify an entity with a SYSTEM tag.

References:
http://tomcat.apache.org/security-4.html
http://tomcat.apache.org/security-5.html
http://tomcat.apache.org/security-6.html

Mozilla Firefox Multiple Vulnerabilities

“Disclose sensitive information; Conduct phishing attacks; Manipulate data”

Some vulnerabilities and a weakness have been reported in Mozilla Firefox, which can be exploited by malicious people to disclose sensitive information, conduct phishing attacks, manipulate certain data, and potentially compromise a user's system.

1) Various errors in the browser engine can be exploited to cause a memory corruption.

2) Various errors in the Javascript engine can be exploited to cause a memory corruption.

Successful exploitation of these vulnerabilities may allow execution of arbitrary code.

3) An error in the handling of onUnload events can be exploited to read and manipulate the document's location of new pages.

4) Input passed to the user ID when making an HTTP request using Digest Authentication is not properly sanitized before being used in a request. This can be exploited to insert arbitrary HTTP headers into a user's request when a proxy is used.

5) An error when displaying web pages written in the XUL markup language can be exploited to hide the window's title bar and facilitate phishing attacks.

6) An error exists in the handling of "smb:" and "sftp:" URI schemes on Linux systems with gnome-vfs support. This can be exploited to read any file owned by the target user via a specially crafted page on the same server.

Successful exploitation requires that the attacker has write access to a mutually accessible location on the target server and the user is tricked into loading the malicious page.

7) An unspecified error in the handling of "XPCNativeWrappers" can lead to execution of arbitrary Javascript code with the user's privileges via subsequent access by the browser chrome (e.g. when a user right-clicks to open a context menu).

References:
http://www.mozilla.org/security/announce/2007/mfsa2007-29.html
http://www.mozilla.org/security/announce/2007/mfsa2007-30.html
http://www.mozilla.org/security/announce/2007/mfsa2007-31.html
http://www.mozilla.org/security/announce/2007/mfsa2007-33.html
http://www.mozilla.org/security/announce/2007/mfsa2007-34.html
http://www.mozilla.org/security/announce/2007/mfsa2007-35.html
http://www.mozilla.org/security/announce/2007/mfsa2007-36.html

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