netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 41

October 19, 2007

Table of Contents

Product Focus

ASN.1 Vulnerability Scanner – The ASN.1 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 MS04-007 that could allow remote code execution.

This Week in Review

SMB's underestimate the consequences. Europe plans ban on bomb making websites. Attackers bypass firewalls on wi-fi.New report from StopBadWare group.

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

- **Most Small and Mid-Sized Businesses Worldwide are Exposed to the Growing Wave of Internet Security Threats**

Seven Out of 10 SMBs Worldwide Reported Spyware and Virus Infections but Underestimate the Consequences. Global Economic Engine Vulnerable to Cyber Crime.
Webroot Software, Inc., a leading provider of Internet security software for the consumer, enterprise and SMB markets, today unveiled its latest report, "State of Internet Security: Protecting Small and Medium Businesses". The report highlights

startling survey results surrounding Internet security threats among SMBs worldwide. In conjunction with the report, Webroot has released a handbook for SMBs, "A Guide to Security for Small & Medium Business" that provides tips and best practices for protecting technology infrastructure and sensitive customer data from malware and cyber criminals.

CRMToday

Full Story :
http://www.crm2day.com/news/crm/123700.php

❖ EU plans ban on bomb-making info on websites

Part of imminent 'ambitious counter terrorism package'
European Union Justice, Freedom (sic) & Security Commissioner Franco Frattini yesterday turned up the volume on terror threats, ahead of the EU's adoption of "an ambitious counter terrorism package" next month. Terrorists, said Frattini, seek new technology, could deploy bioterrorism with devastating effect, and if they got hold of weapons of mass destruction "the consequences would be catastrophic."

Terrorists themselves have so far shown little sign of either a bioterror or nuclear holocaust delivery capability, confining themselves in the main to hopeless poison plots and loopy fantasies involving smoke detectors and similar, but as they say, often while they're saying "the consequences would be catastrophic", "it's only a matter of time before...

The Register

Full Story :
http://www.theregister.co.uk/2007/10/19/frattini_terror_measure_package/

❖ Wi-fi security system is 'broken'

More holes have been picked in the security measure designed to protect the privacy and data of wi-fi users.
The latest attack lets criminals defeat firewalls and spy on where someone goes and what they do online.

It comes after a series of other attacks that, experts say, have left the basic protection in wi-fi comprehensively "broken".

But compatibility issues mean that many will have no alternative but to use the much weakened protection system.

Bbc news

Full Story :
http://news.bbc.co.uk/1/hi/technology/7052223.stm

❖ Official: the web has an evil side

New report finds plenty to terrify.
It's getting harder and harder to know who to trust on the Web, according to online safety advocates StopBadware.org.
On Tuesday, the group released its 2007 Trends in Badware report, saying the bad guys are finding new ways to place their malicious software on our computers - often by compromising Web sites that we trust.

With the help of one of its sponsor companies, Google, StopBadware maintains a list of 200,000 Web sites that are known to be associated with malicious downloads. According to Max Weinstein, a project manager with StopBadware, more than half of these sites have been hacked and don't even realise it.

techworld

Full Story :
http://www.techworld.com/security/features/index.cfm?featureID=3738&pagtype=samecatsamechan

New Vulnerabilities Tested in SecureScout

- **13569 Oracle Database Server - Workspace Manager component unspecified Vulnerability (oct-2007/DB10)**

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

CVE Reference: CVE-2007-5510

- **13568 Oracle Database Server - Workspace Manager component unspecified Vulnerability (oct-2007/DB09)**

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

CVE Reference: CVE-2007-5510

❖ 13567 Oracle Database Server - Workspace Manager component unspecified Vulnerability (oct-2007/DB08)

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

CVE Reference: CVE-2007-5510

❖ 13566 Oracle Database Server - Spatial component unspecified Vulnerability (oct-2007/DB07)

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

The issue is fixed in VMware Server 1.0.4 Build 56528.

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

❖ 13565 Oracle Database Server - Spatial component unspecified Vulnerability (oct-2007/DB06)

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-2007-5509

❖ 13564 Oracle Database Server - Oracle Text component unspecified Vulnerability (oct-2007/DB05)

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

❖ 13563 Oracle Database Server - Oracle Text component unspecified Vulnerability (oct-2007/DB04)

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

❖ 13562 An unspecified vulnerability with unknown impact exists in Oracle Database Server Oracle Text component.

A spoofing vulnerability exists in Internet Explorer that could allow an attacker to display spoofed content in a browser window. The address bar and other parts of the trust UI has been navigated away from the attacker's Web site but the content of the window still contains the attacker's Web page.

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

References:

* BUGTRAQ: 20071017 Multiple SQL Injection Flaws in Oracle CTX_DOC package
http://www.securityfocus.com/archive/1/archive/1/482425/100/0/threaded
* MISC:
http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-oracle-ctx-doc/
* 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: 26101
http://www.securityfocus.com/bid/26101
* 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-2007-5508

❖ 13561 Oracle Database Server - Export component unspecified Vulnerability (oct-2007/DB02)

An unspecified vulnerability with unknown impact exists in Oracle Database Server Export 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

❖ 13560 Oracle Database Server - Import component unspecified Vulnerability (oct-2007/DB01)

An unspecified vulnerability with unknown impact exists in Oracle Database Server Import 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

New Vulnerabilities found this Week

Oracle Products Multiple Vulnerabilities

"Disclose sensitive information; SQL injection attacks; Denial of Service"

Multiple vulnerabilities have been reported for various Oracle products. Some have unknown impacts, others can be exploited to disclose sensitive information, conduct SQL injection attacks, or to cause a DoS (Denial of Service).

References:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html
http://descriptions.securescout.com/tc/13560
http://descriptions.securescout.com/tc/13561
http://descriptions.securescout.com/tc/13562
http://descriptions.securescout.com/tc/13563
http://descriptions.securescout.com/tc/13564
http://descriptions.securescout.com/tc/13565
http://descriptions.securescout.com/tc/13566
http://descriptions.securescout.com/tc/13567
http://descriptions.securescout.com/tc/13568
http://descriptions.securescout.com/tc/13569

Opera Multiple Vulnerabilities

"Cross-site scripting"

Some vulnerabilities have been reported in Opera, where one vulnerability has an unknown impact and others can be exploited by malicious people to conduct cross-site scripting attacks and to compromise a user's system.

1) Opera may launch external email or newsgroup clients incorrectly. This can be

exploited to execute arbitrary commands by e.g. visiting a malicious website.

Successful exploitation requires that the user has configured an external email or newsgroup client.

2) An error when processing frames from different websites can be exploited to bypass the same-origin policy. This allows to overwrite functions of those frames and to execute arbitrary HTML and script code in a user's browser session in context of other sites.

3) An unspecified error exists in Opera in combination with Adobe Flash Player 9.0.47.0 and earlier on Mac OS X. No further information is currently available.

The vulnerabilities are reported in all versions of Opera for Desktop prior to version 9.24.

References:
http://www.opera.com/support/search/view/866/
http://www.opera.com/support/search/view/867/
http://www.opera.com/support/search/view/868/

Cisco Unified Communications Manager Two Vulnerabilities

"Denial of Service"

Two vulnerabilities have been reported in Cisco Unified Communications Manager (CUCM), which can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system.

1) A boundary error in the Centralized TFTP File Locator Service of CUCM TFTP when processing filenames can be exploited to cause a buffer overflow.

Successful exploitation may allow execution of arbitrary code.

2) An error when processing SIP INVITE messages can be exploited to cause a resource exhaustion by e.g. flooding a CUCM system with SIP INVITE messages to default port 5060/UDP.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20071017-cucm.shtml

Winamp FLAC Media File Processing Integer Overflows

"Arbitrary code execution"

Some vulnerabilities have been reported in Winamp, which can be exploited by malicious people to compromise a user's system.

The vulnerabilities are reported in version 5.35. Other versions may also be affected.

References:
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=608

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