netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 43

October 27, 2006

Table of Contents

Product Focus

This Week in Review

Top Security News Stories this Week

New Vulnerabilities Tested in SecureScout

New Vulnerabilities found this Week

Product Focus

Sapphire Worm Scanner – The Sapphire Worm 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 SQL buffer overflow vulnerability (MS02-039/MS02-061) that the recent Sapphire Worm uses to propagate.

This Week in Review

Free honeypot for Windows from netVigilance. Public key turns 30. Tech challenges legal systems. Information Security has come a long way.

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

- **NetVigilance offers a free Windows honeypot**

Network vulnerability-assessment vendor NetVigilance is offering a free tool called WinHoneyd as a low-interaction honeypot that can mimic aspects of a Windows-based network to be used as an attack decoy.
The intent of the WinHoneyd honeypot, says NetVigilance CEO Jesper Jurcenoks, is to emulate the real corporate network, either at the Internet edge or deep inside the LAN, by means of a honeypot so the impact of attacks can be better understood.

“As soon as you have a guy probing your fake server, you can use this information to create better countermeasures,” said Jurcenoks. “The honeypot can be a way to learn about new attacks.”

He said Winhoneyd is a simple command-line tool that can emulate thousands of different Windows-based desktops and servers, and users can optionally add information by proxy or otherwise to give the look of a real corporate computer.

Network World

Full Story :
http://www.networkworld.com/news/2006/102506-netvigilance-honeypot.html

- **Public key cryptography celebrates anniversary**

Computer security dignitaries hail the security technology's birth, tied to November 1976 paper

MOUNTAIN VIEW, Calif. -- Dignitaries from the computer security field took the stage at the Computer History Museum Thursday evening to note the 30th anniversary of public key cryptography and wax historical about academic, governmental and commercial developments in security and ponder the future.
Panelists included persons such as Whitfield Diffie, who is a cryptography pioneer and chief security officer at Sun Microsystems; Notes founder Ray Ozzie, now Microsoft's chief software architect, and Brian Snow, retired director for the National Security Agency's Information Assurance Directorate. They touched on a broad array of topics ranging from NSA obstacles and export regulations to decades-old research papers and the Clipper chip.

The concept of public key cryptography has evolved over the years and its principles are being extended into areas such as e-commerce, panelists noted. Public key cryptography uses public and private keys between sender and recipient of a message for security purposes. The sender encrypts a message with a public key and the recipient uses a private key to decrypt it. Its birth is traced to the November 1976 publishing of a paper entitled, "New Directions in Cryptography," by Diffie and Martin Hellman, who also served on Thursday's panel and is a Stanford University professor.

Infoworld

Full Story :
http://www.infoworld.com/article/06/10/27/HNcrypto_1.html?source=rss&url=http://www.infoworld.com/article/06/10/27/HNcrypto_1.html

- **Tech presents legal system with 'tremendous curves'**

VOIP, botnets among challenges cyberprotectors face
October 27, 2006 (Network World) -- A legal system rife with outdated laws never designed to cope with such new technologies as VOIP is just one of the worries facing Stephen Treglia, chief of the technology crime unit in the district attorney's office of New York's Nassau County.

"This has been a tremendous curve for the legal system to adapt to," said Treglia at this week's InfoSecurity conference, where he and other experts discussed how they try to cope with multiple challenges, such as the botnet threat, controlling hackers and devising cost-effective ways to maintain voice and data communications during emergencies. He said federal and state lawmakers have had a hard time keeping up with the enormous technical changes brought about by IP-based communications and the Web.

"For instance, we really have had no hacking statute in New York until the one that goes into effect by the end of the year," Treglia said. Another important law that takes effect in New York this year is the New York Information Security Breach and Notification Act, which requires a person or business operating in New York to disclose a confirmed or even suspected computer-security breach of private information -- Social Security number, driver's license or account numbers and credit and debit card numbers in combination with any required security codes.

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9004500&taxonomyId=17&intsrc=kc_top

- **Information security means better business**

Information security, as a recognised business activity, has come a long way in the past decade. Various factors have caused the discipline to mature and it has now attained its "licence to operate" within the corporate and public sector environments, becoming one of the core business and organisational enablers.
there is little room for error, as the consequences of insecure systems and information are almost always costly and distracting.

The challenge now for senior security specialists is to develop an ongoing dialogue with the board about the importance of information security in the context of organisational goals.

Information is the engine of global enterprise, and fit-for-purpose information security is fundamental to managing global enterprise risk. The regulatory environment, especially the requirements of Sarbanes-Oxley, has pushed security onto the board's agenda.

Computerweekly.com

Full Story :
http://www.computerweekly.com/Articles/2006/10/27/219436/Information+security++means+better+business.htm

New Vulnerabilities Tested in SecureScout

- **13448 Oracle Database Server - Oracle Spatial component SQL Injection Vulnerability (oct-2006/DB12)**

An SQL Injection exists in COMPRESSDATA. Fixed Compress.class

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html

Other references:
http://www.databasesecurity.com/oracle/OracleOct2006-CPU-Analysis.pdf
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html

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

CVE Reference: CVE-2006-5335

- **13449 Oracle Database Server - Oracle Spatial component SQL Injection Vulnerability (oct-2006/DB13)**

The package MDSYS.SDO_LRS contains a SQL injection vulnerability in the first parameter of convert_to_lrs_layer. Oracle forgot to fix this problem with the April CPU. Oracle fixed these vulnerabilities with the package DBMS_ASSERT. To exploit this vulnerability it is necessary to have the privilege to create a PL/SQL-function.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html

Other references:
http://www.databasesecurity.com/oracle/OracleOct2006-CPU-Analysis.pdf
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html
http://www.red-database-security.com/advisory/oracle_sql_injection_sdo_lrs.html

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

CVE Reference: CVE-2006-5340

❖ 13450 Oracle Database Server - XMLDB component SQL Injection Vulnerability (oct-2006/DB14)

An SQL Injection exists in PITRIG_DROP and PITRIG_DROPMETADATA. PITRIG_DROP is called from the XDB.XDB_PI_TRIG trigger.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html

Other references:
http://www.databasesecurity.com/oracle/OracleOct2006-CPU-Analysis.pdf
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html

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

CVE Reference: CVE-2006-5341

❖ 13451 Oracle Database Server - XMLDB component SQL Injection Vulnerability (oct-2006/DB15)

An SQL Injection exists in DISABLE_HIERARCHY_INTERNAL.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html

Other references:
http://www.databasesecurity.com/oracle/OracleOct2006-CPU-Analysis.pdf
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html
http://www.red-database-security.com/advisory/oracle_sql_injection_dbms_xdbz0.html

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

CVE Reference: CVE-2006-5341

❖ 13452 Oracle Database Server - Change Data Capture (CDC) component SQL Injection Vulnerability (oct-2006/DB16)

An SQL Injection exists in SUBSCRIBE. Fixed validateViewName in Subscribe.class.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html

Other references:
http://www.databasesecurity.com/oracle/OracleOct2006-CPU-Analysis.pdf
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html

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

CVE Reference: CVE-2006-5335

❖ 13453 Oracle Database Server - Oracle Spatial component SQL Injection Vulnerability (oct-2006/DB17)

An SQL Injection exists in trigger.

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

References:

References:
Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html

Other references:
http://www.databasesecurity.com/oracle/OracleOct2006-CPU-Analysis.pdf
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html

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

CVE Reference: CVE-2006-5340

❖ 13454 Oracle Database Server - Oracle Spatial component unspecified Vulnerability (oct-2006/DB18)

An unspecified vulnerability exists in Oracle Spatial component.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html

Other references:
http://www.databasesecurity.com/oracle/OracleOct2006-CPU-Analysis.pdf
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html

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

CVE Reference: CVE-2006-5342

❖ 13455 Oracle Database Server - Database Scheduler component unspecified Vulnerability (oct-2006/DB19)

An unspecified vulnerability exists in Database Scheduler component.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html

Other references:
http://www.databasesecurity.com/oracle/OracleOct2006-CPU-Analysis.pdf
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html

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

CVE Reference: CVE-2006-5343

❖ 14049 DNS server allows Cache Snooping

If the DNS server allows cache snooping, an attacker could potentially determine if a Resource Record is (or not) present in the server cache.

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

References:

Research Paper:
http://www.sysvalue.com/papers/DNS-Cache-Snooping/

Other references:
http://www.securityspace.com/smysecure/catid.html?id=12217
http://www.securityfocus.com/archive/112/361106/30/0/threaded
http://www.secuobs.com/plugs/12217.shtml

http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020436.html

CVE Reference:

❖ **17735 Raptor FW version 6.5 detection (HTTP Proxy)**

By sending an invalid HTTP request to a webserver behind Raptor firewall, the http proxy itself will respond and diclose its identity.

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

References:

http://www.nessus.org/plugins/index.php?view=single&id=10730
http://secunia.com/product/513/

CVE Reference:

New Vulnerabilities found this Week

Winamp Lyrics3 and Ultravox Processing Buffer Overflows

"Buffer overflow"

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

1) An error in the Ultravox protocol handler during processing of the "ultravox-max-msg" header can be exploited to cause a heap-based buffer overflow via either a specially crafted playlist or a "shout:" or "uvox:" URI.

2) An error during the parsing of certain Lyrics3 tags can be exploited to cause a heap-based buffer overflow via either a specially crafted playlist or a "shout:" or "uvox:" URI.

The vulnerabilities are reported in versions 2.666 through 5.3.

References:
http://www.winamp.com/player/version_history.php#5.31
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=431
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=432

Internet Explorer 7 Popup Address Bar Spoofing Weakness

"Phishing attacks"

A weakness has been discovered in Internet Explorer, which can be exploited by malicious people to conduct phishing attacks.

The problem is that it's possible to display a popup with a somewhat spoofed address bar where a number of special characters have been appended to the URL. This makes it possible to only display a part of the address bar, which may trick users into performing certain unintended actions.

The weakness is confirmed in Internet Explorer 7 on a fully patched Windows XP SP2 system.

References:
http://secunia.com/advisories/22542/

Internet Explorer 7 "mhtml:" Redirection Information Disclosure

"Disclose potentially sensitive information"

A vulnerability has been discovered in Internet Explorer, which can be exploited by malicious people to disclose potentially sensitive information.

The vulnerability is caused due to an error in the handling of redirections for URLs with the "mhtml:" URI handler. This can be exploited to access documents served from another web site.

The vulnerability has been confirmed on a fully patched system with Internet Explorer 7.0 and Microsoft Windows XP SP2. Other versions may also be affected.

References:
http://secunia.com/advisories/22477/

AOL YGPPDownload ActiveX Control Buffer Overflows

"Execution of arbitrary code"

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

1) A boundary error in the YGPPDownload ActiveX control (YGPPicDownload.dll) when processing input passed to the "AddPictureNoAlbum()" method can be exploited to cause a heap-based buffer overflow.

2) A boundary error in the YGPPDownload ActiveX control (YGPPicDownload.dll) when processing input passed to the "downloadFileDirectory" property can be exploited to cause a heap-based buffer overflow.

Successful exploitation of the vulnerabilities allows execution of arbitrary code.

The vulnerabilities are reported in AOL Security Edition 9.0 with downloader plugin version 9.2.3.0. Other versions may also be affected.

References:
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=429
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=430

PostgreSQL Denial of Service Vulnerabilities

"Denial of Service"

Some vulnerabilities have been reported in PostgreSQL, which can be exploited by malicious users to cause a DoS (Denial of Service).

1) An incorrect type check before coercing unknown literals into the ANYARRAY type can be exploited to cause a crash when converting certain literals into ANYARRAY.

2) An error exists within the handling of aggregate functions in UPDATE statements, which can be exploited to crash the server backend.

3) An error within the logging of V3-protocol execute messages of ROLLBACK or COMMIT statements can be exploited to cause a crash.

References:
http://www.postgresql.org/about/news.664
http://projects.commandprompt.com/public/pgsql/changeset/26457
http://projects.commandprompt.com/public/pgsql/changeset/25504
http://projects.commandprompt.com/public/pgsql/changeset/25953

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