netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 3

January 19, 2007

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

Sasser Worm Scanner – The Sasser 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 SSL Vulnerability (MS04-011) that used by the Sasser Worm to infect machines.

netVigilance, Inc is proud to announce that we have been awarded the Payment Card Industry (PCI) Certifications as "Approved Scanning Vendor" (ASV).
This Certification allows netVigilance, Inc to determine PCI Data Security Standard (DSS) Compliance for vendors accepting Credit Cards on a worldwide basis.

SANS version 7 (November 2006) support has been added to the SecureScout products.

This Week in Review

When the big assault occurs. Beware of 'Free WiFi' scam in US airports. Group established to work on 'Code of Conducts'. Spammers take advantage of recent European storm.

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

- **A tale of two Internets**

Creating a verified, authenticated alternative to today's Internet would be good for

business -- and everyone's overall security
One third of all U.S. adults had their identity and financial information stolen or lost in 2006 alone. Bogus messages make up 90 percent of the e-mail traffic on the Internet. Ninety-nine percent of all malware exists to steal your money. Tens of millions of dollars are being stolen off the Internet every day from bank fraud, phishing attacks, bogus stock trades, extortion, etc. A large percentage of the Internet is owned and operated by the criminals, and they almost never get caught.

No, the sky isn't falling. It fell a long time ago.

In the future, there will be a huge Internet crime theft. The loss will total in the billions of dollars after a single hour. When it is through, it will interrupt the Internet, the banking system, and business in general for a week or more as we struggle to find out how it happened. Our resolve and trust in our money being stored in electronic bits will be tested.

Why am I so sure it will happen? Because we've got human greed on one side and passive indifference on the other.

InfoWorld

Full Story :
http://www.infoworld.com/article/07/01/19/04OPsecadvise_1.html?source=rss&url=http://www.infoworld.com/article/07/01/19/04OPsecadvise_1.html

- **Don't fall victim to the 'Free Wi-Fi' scam**

Those wireless connections could be a trap
The next time you're at an airport looking for a wireless hot spot, and you see one called "Free Wi-Fi" or a similar name, beware -- you may end up being victimized by the latest hot-spot scam hitting airports across the country.

You could end up being the target of a "man in the middle" attack, in which a hacker is able to steal the information you send over the Internet, including usernames and passwords. And you could also have your files and identity stolen, end up with a spyware-infested PC and have your PC turned into a spam-spewing zombie. The attack could even leave your laptop open to hackers every time you turn it on, by allowing anyone to connect to it without your knowledge.

If you're a Windows Vista user, you're especially susceptible to this attack because of the difficulty in identifying it when using Vista. In this article, you'll learn how the attack works and how to keep yourself safe from it if you use Windows XP or Vista.

ComputerWorld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9008399&taxonomyId=17&intsrc=kc_feat

- **Microsoft, Google to work on free speech, privacy rights**

Four tech companies to work with rights groups on code of conduct
Microsoft Corp., Google Inc. and two other technology companies said today that they will develop a code of conduct with a coalition of nongovernmental organizations to promote freedom of expression and privacy rights.

Microsoft and Google, along with Yahoo Inc. and Vodafone Group PLC, said the new guidelines are the result of talks with Business for Social Responsibility and the Berkman Center for Internet & Society at Harvard Law School.

Technology companies have come under fire for providing equipment or software that permits governments to censor information or monitor the online or offline activities of their citizens. For example, last year, Google was criticized over its creation of a censored, local version of its search engine for the China market.

ComputerWorld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9008544&taxonomyId=17&intsrc=kc_top

- **Inboxes battered by Trojan spam deluge**

Virus writers are taking advantage of the winter storms ravaging Northern Europe to launch a malware blitz of their own.

The attack attempts to trick users into executing malicious files containing Trojan horse code, that pose as information about the inclement weather. The Trojans are being distributed in messages with subject lines such as "230 dead as storm batters Europe", and infectious attachments containing the Small-DAM (AKA DwnLdr-FYD) Trojan. Attachments may contain one of the following filenames: Full Clip.exe; Full Story.exe; Read More.exe and Video.exe.

If executed, the payload turns infected machines into compromised, zombie clients under the control of hackers.

TheRegister

Full Story :
http://www.theregister.co.uk/2007/01/19/trojan_storm/

New Vulnerabilities Tested in SecureScout

- **13509 Oracle Database Server - Advanced Queuing component SQL Injection Vulnerability (jan-2007/DB01)**

An SQL Injection vulnerability exists in Oracle Database Server Advanced Queuing component.

The issue affects the system confidentiality and integrity.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_jan_2007.html
http://www.red-database-security.com/advisory/oracle_sql_injection_dbms_aq_inv.html

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

CVE Reference: CVE-2007-0268

❖ 13510 Oracle Database Server - Change Data Capture component SQL Injection Vulnerability (jan-2007/DB02)

An SQL Injection vulnerability exists in Oracle Database Server Change Data Capture component.

The issue affects the system confidentiality and integrity.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_jan_2007.html

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

CVE Reference: CVE-2007-0269

❖ 13511 Oracle Database Server - Data Guard component Buffer Overflow Vulnerability (jan-2007/DB03)

A Buffer Overflow vulnerability exists in Oracle Database Server Data Guard component.

The issue affects the system integrity and availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_jan_2007.html

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

CVE Reference: CVE-2007-0270

❖ 13512 Oracle Database Server - Log Miner component Buffer Overflow Vulnerability (jan-2007/DB04)

A Buffer Overflow vulnerability exists in Oracle Database Server Log Miner component.

The issue affects the system integrity and availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_jan_2007.html

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

CVE Reference: CVE-2006-4333

❖ 13513 Oracle Database Server - Oracle Spatial component Buffer Overflow Vulnerability (jan-2007/DB05)

A Buffer Overflow vulnerability exists in Oracle Database Server Oracle Spatial component.

The issue affects the system integrity and availability.

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

References:

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

updates/cpujan2007.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_jan_2007.html

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

CVE Reference: CVE-2007-0272

❖ 13514 Oracle Database Server - XMLDB component Buffer Overflow Vulnerability (jan-2007/DB06)

A Buffer Overflow vulnerability exists in Oracle Database Server XMLDB component.

The issue affects the system integrity.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_jan_2007.html
http://www.red-database-security.com/advisory/oracle_xmldb_css2.html

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

CVE Reference: CVE-2007-0273

❖ 13515 Oracle Database Server - Advanced Replication component Buffer Overflow Vulnerability (jan-2007/DB07)

A Buffer Overflow vulnerability exists in Oracle Database Server Advanced Replication component.

The issue affects the system availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_jan_2007.html

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

CVE Reference: CVE-2007-0268

❖ 13516 Oracle Database Server - Export component Buffer Overflow Vulnerability (jan-2007/DB08)

A Buffer Overflow vulnerability exists in Oracle Database Server Export component.

The issue affects the system availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_jan_2007.html

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

CVE Reference: CVE-2007-0274

❖ 13517 Oracle Database Server - Oracle Streams component Buffer Overflow Vulnerability (jan-2007/DB09)

A Buffer Overflow vulnerability exists in Oracle Database Server Oracle Streams component.

The issue affects the system availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_jan_2007.html

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

CVE Reference: CVE-2007-0274

❖ **13518 Oracle Database Server - Advanced Security Option component Buffer Overflow Vulnerability (jan-2007/DB09)**

A Buffer Overflow vulnerability exists in Oracle Database Server Advanced Security Option component.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_jan_2007.html

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

CVE Reference: CVE-2007-0276

New Vulnerabilities found this Week

Oracle Products Multiple Vulnerabilities

"Gain access to sensitive information; Denial of Service; Cross-site scripting; SQL injection attacks"

Multiple vulnerabilities have been reported in various Oracle products. Some of these vulnerabilities have unknown impacts while others can be exploited to gain access to sensitive information, cause a DoS (Denial of Service), conduct cross-site scripting and SQL injection attacks, and potentially compromise a vulnerable system.

References:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html
http://www.red-database-security.com/advisory/oracle_buffer_overflow_ons.html
http://www.red-database-security.com/advisory/oracle_xmldb_css2.html
http://www.red-database-security.com/advisory/oracle_sql_injection_dbms_aq_inv.html

http://descriptions.securescout.com/tc/13509
http://descriptions.securescout.com/tc/13510
http://descriptions.securescout.com/tc/13511
http://descriptions.securescout.com/tc/13512
http://descriptions.securescout.com/tc/13513
http://descriptions.securescout.com/tc/13514
http://descriptions.securescout.com/tc/13515
http://descriptions.securescout.com/tc/13516
http://descriptions.securescout.com/tc/13517
http://descriptions.securescout.com/tc/13518

Sun Java JRE GIF Image Processing Buffer Overflow Vulnerability
"Execution of arbitrary code"

A vulnerability has been reported in Sun Java Runtime Environment (JRE), which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an error when processing GIF images and can be exploited to cause a heap-based buffer overflow via a specially crafted GIF image with an image width of 0.

Successful exploitation allows execution of arbitrary code.

The vulnerability is reported in the following versions:
* JDK and JRE 5.0 Update 9 and prior.
* SDK and JRE 1.4.2_12 and prior.
* SDK and JRE 1.3.1_18 and prior.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102760-1
http://www.zerodayinitiative.com/advisories/ZDI-07-005.html
http://www.kb.cert.org/vuls/id/388289

Squid Denial of Service Vulnerabilities
"Denial of Service"

Two vulnerabilities have been reported in Squid, which can be exploited by malicious people to cause a DoS (Denial of Service).

1) An error in the handling of certain FTP URL requests can be exploited to crash Squid by visiting a specially crafted FTP URL via the proxy.

2) An error in the external_acl queue can cause Squid to crash when it is under high load conditions.

The vulnerabilities are reported in version 2.6. Other versions may also be affected.

References:
http://www.squid-cache.org/Versions/v2/2.6/squid-2.6.STABLE7-RELEASENOTES.html#s12

oftpd LPSV and LPRT Denial of Service Vulnerability
"Denial of Service"

Tavis Ormandy has reported a vulnerability in oftpd, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error within the handling of LPSV and LPRT commands. This can be exploited to trigger an assertion error by passing specially crafted arguments to the LPSV or LPRT commands, which causes oftpd to abort.

The vulnerability is reported in version 0.3.7. Other versions may also be affected.

References:

http://www.gentoo.org/security/en/glsa/glsa-200701-09.xml

FreeBSD UFS "ufs_dirbad()" Local Denial of Service
"Denial of Service"

LMH has reported a vulnerability in FreeBSD, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

The vulnerability is caused due to an error within the "ufs_dirbad()" function when handling corrupted UFS images and can be exploited to cause a kernel panic.

The vulnerability is reported in FreeBSD 6.1. Other versions may also be affected.

References:
http://projects.info-pull.com/moab/MOAB-12-01-2007.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