netVigilance

ScoutNews Team **February 10, 2006**
2006 Issue # 6

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Islamic hacker launch Jihad against Danish websites, Linus Torvalds eludes to break with latest GPL license, warnings from Nortel boss on VOIP security and are Googles eyes getting too big?

Enjoy reading

Call or email netVigilance to get an update on SecureScout.
(503) 524 5758 or sales@netVigilance.com

Top Security News Stories this Week

- **Danish websites hacked in cartoon blowup**

F-Secure and Zone-h.org have catalogued between 500 and 600 Danish websites that have been defaced with anti-Danish or pro-Islamic messages and threats.

TechWeb

Related Links :
http://www.techweb.com/wire/ebiz/179101384%3bjsessionid=05HKIDQOYTMS4QSNDBNCKHSCJUMEKJVN
http://www.tgdaily.com/2006/02/10/danishwebsites_hacked/

- **Torvalds speaks out against GPL anti-DRM measures**

Linus Torvalds posted a statement to the Linux mailing list that a proposed update to the General Public Licence (GPL), could in fact undermine computer security.

The father of Linux said that he plans to keep Linux under the current version 2 of the GPL based on his assertion where he believes it's appropriate for secret digital keys to be used to sign software. The Free Software Foundation wishes to revise the upcoming GPLv3 to add what they term 'anti-DRM' measures.

Silicon.com

Full Story :
http://www.silicon.com/research/specialreports/opensource/0,3800004943,39156200,00.htm

- **Nortel CEO describes vulnerability of all-digital phone network**

Bill Owens, chief executive of Nortel Networks raised concerns that the new voice communications networks, based on internet protocol, are vulnerable to viruses, worms and hacker attacks.

Mr. Owens warns that common worms such as Mytob for example, could not only wreak hovoc not only on computer networks but now voice networks as well.

Financial Times

Full Story :
http://news.ft.com/cms/s/15709092-2a01-11da-b890-00000e2511c8.html

- **Digital Rights advocates call for Google boycott**

The Electronic Frontier Foundation issued a warning to users that the latest version of Google Desktop actually stores the contents of a user's hard drive on Google servers.

The new "Search Across Computers" feature which allows users to search the contents of one computer from a separate computer. The EFF wants consumers to be aware that their personal data vulnerable to government subpoena, private litigants, and hackers.

RedHerring

Related Links :
http://www.redherring.com/Article.aspx?a=15669&hed=Google+Desktop+Boycott+Urged&sector=Industries&subsector=SecurityAndDefense

New Vulnerabilities Tested in SecureScout

- **13343 Oracle Database Server - Query Optimizer component Unspecified error (jan-2006/DB19)**

An unspecified error in the Query Optimizer component can potentially be exploited to gain knowledge of certain information, overwrite arbitrary files, and to conduct SQL injection attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html
http://www.red-database-security.com/advisory/oracle_tde_wallet_password.html
http://www.red-database-security.com/advisory/oracle_tde_unencrypted_sga.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft_int.html
http://www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
http://www.red-database-security.com/advisory/oracle_reports_read_any_xml_file.html
http://www.imperva.com/application_defense_center/papers/oracle-dbms-01172006.html

Other references:
http://secunia.com/advisories/16092/
http://www.kb.cert.org/vuls/id/150332
http://www.kb.cert.org/vuls/id/545804
http://www.kb.cert.org/vuls/id/870172
http://www.kb.cert.org/vuls/id/871756
http://www.kb.cert.org/vuls/id/891644
http://www.kb.cert.org/vuls/id/983340
http://www.kb.cert.org/vuls/id/999268

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

CVE Reference: None

- **13344 Oracle Database Server - Query Optimizer component Unspecified error (jan-2006/DB20)**

An unspecified error in the Query Optimizer component can potentially be exploited to gain knowledge of certain information, overwrite arbitrary files, and to conduct SQL injection attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html
http://www.red-database-security.com/advisory/oracle_tde_wallet_password.html
http://www.red-database-security.com/advisory/oracle_tde_unencrypted_sga.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft_int.html
http://www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
http://www.red-database-security.com/advisory/oracle_reports_read_any_xml_file.html
http://www.imperva.com/application_defense_center/papers/oracle-dbms-01172006.html

Other references:
http://secunia.com/advisories/16092/
http://www.kb.cert.org/vuls/id/150332
http://www.kb.cert.org/vuls/id/545804
http://www.kb.cert.org/vuls/id/870172
http://www.kb.cert.org/vuls/id/871756
http://www.kb.cert.org/vuls/id/891644
http://www.kb.cert.org/vuls/id/983340
http://www.kb.cert.org/vuls/id/999268

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

CVE Reference: None

❖ 13345 Oracle Database Server - Security component Unspecified error (jan-2006/DB21)

An unspecified error in the Security component can potentially be exploited to gain knowledge of certain information, overwrite arbitrary files, and to conduct SQL injection attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html
http://www.red-database-security.com/advisory/oracle_tde_wallet_password.html
http://www.red-database-security.com/advisory/oracle_tde_unencrypted_sga.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft_int.html
http://www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
http://www.red-database-security.com/advisory/oracle_reports_read_any_xml_file.html
http://www.imperva.com/application_defense_center/papers/oracle-dbms-

01172006.html

Other references:
http://secunia.com/advisories/16092/
http://www.kb.cert.org/vuls/id/150332
http://www.kb.cert.org/vuls/id/545804
http://www.kb.cert.org/vuls/id/870172
http://www.kb.cert.org/vuls/id/871756
http://www.kb.cert.org/vuls/id/891644
http://www.kb.cert.org/vuls/id/983340
http://www.kb.cert.org/vuls/id/999268

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

CVE Reference: None

❖ 13346 Oracle Database Server - Streams Apply component Unspecified error (jan-2006/DB22)

An unspecified error in the Streams Apply component can potentially be exploited to gain knowledge of certain information, overwrite arbitrary files, and to conduct SQL injection attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html
http://www.red-database-security.com/advisory/oracle_tde_wallet_password.html
http://www.red-database-security.com/advisory/oracle_tde_unencrypted_sga.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft_int.html
http://www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
http://www.red-database-security.com/advisory/oracle_reports_read_any_xml_file.html
http://www.imperva.com/application_defense_center/papers/oracle-dbms-01172006.html

Other references:
http://secunia.com/advisories/16092/
http://www.kb.cert.org/vuls/id/150332
http://www.kb.cert.org/vuls/id/545804
http://www.kb.cert.org/vuls/id/870172
http://www.kb.cert.org/vuls/id/871756
http://www.kb.cert.org/vuls/id/891644
http://www.kb.cert.org/vuls/id/983340
http://www.kb.cert.org/vuls/id/999268

Product Homepage:

http://www.oracle.com/

CVE Reference: None

❖ 13347 Oracle Database Server - Streams Capture component Unspecified error (jan-2006/DB23)

An unspecified error in the Streams Capture component can potentially be exploited to gain knowledge of certain information, overwrite arbitrary files, and to conduct SQL injection attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html
http://www.red-database-security.com/advisory/oracle_tde_wallet_password.html
http://www.red-database-security.com/advisory/oracle_tde_unencrypted_sga.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft_int.html
http://www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
http://www.red-database-security.com/advisory/oracle_reports_read_any_xml_file.html
http://www.imperva.com/application_defense_center/papers/oracle-dbms-01172006.html

Other references:
http://secunia.com/advisories/16092/
http://www.kb.cert.org/vuls/id/150332
http://www.kb.cert.org/vuls/id/545804
http://www.kb.cert.org/vuls/id/870172
http://www.kb.cert.org/vuls/id/871756
http://www.kb.cert.org/vuls/id/891644
http://www.kb.cert.org/vuls/id/983340
http://www.kb.cert.org/vuls/id/999268

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

CVE Reference: None

❖ 13348 Oracle Database Server - Streams Capture component Unspecified error (jan-2006/DB24)

An unspecified error in the Streams Capture component can potentially be exploited to gain knowledge of certain information, overwrite arbitrary files, and to conduct SQL injection attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html
http://www.red-database-security.com/advisory/oracle_tde_wallet_password.html
http://www.red-database-security.com/advisory/oracle_tde_unencrypted_sga.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft_int.html
http://www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
http://www.red-database-security.com/advisory/oracle_reports_read_any_xml_file.html
http://www.imperva.com/application_defense_center/papers/oracle-dbms-01172006.html

Other references:
http://secunia.com/advisories/16092/
http://www.kb.cert.org/vuls/id/150332
http://www.kb.cert.org/vuls/id/545804
http://www.kb.cert.org/vuls/id/870172
http://www.kb.cert.org/vuls/id/871756
http://www.kb.cert.org/vuls/id/891644
http://www.kb.cert.org/vuls/id/983340
http://www.kb.cert.org/vuls/id/999268

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

CVE Reference: None

❖ 13349 Oracle Database Server - Streams Capture component Unspecified error (jan-2006/DB25)

An unspecified error in the Streams Capture component can potentially be exploited to gain knowledge of certain information, overwrite arbitrary files, and to conduct SQL injection attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html
http://www.red-database-security.com/advisory/oracle_tde_wallet_password.html
http://www.red-database-security.com/advisory/oracle_tde_unencrypted_sga.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft_int.html
http://www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
http://www.red-database-

security.com/advisory/oracle_reports_read_any_xml_file.html
http://www.imperva.com/application_defense_center/papers/oracle-dbms-01172006.html

Other references:
http://secunia.com/advisories/16092/
http://www.kb.cert.org/vuls/id/150332
http://www.kb.cert.org/vuls/id/545804
http://www.kb.cert.org/vuls/id/870172
http://www.kb.cert.org/vuls/id/871756
http://www.kb.cert.org/vuls/id/891644
http://www.kb.cert.org/vuls/id/983340
http://www.kb.cert.org/vuls/id/999268

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

CVE Reference: None

❖ 13350 Oracle Database Server - Streams Subcomponent component Unspecified error (jan-2006/DB26)

An unspecified error in the Streams Subcomponent component can potentially be exploited to gain knowledge of certain information, overwrite arbitrary files, and to conduct SQL injection attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html
http://www.red-database-security.com/advisory/oracle_tde_wallet_password.html
http://www.red-database-security.com/advisory/oracle_tde_unencrypted_sga.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft_int.html
http://www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
http://www.red-database-security.com/advisory/oracle_reports_read_any_xml_file.html
http://www.imperva.com/application_defense_center/papers/oracle-dbms-01172006.html

Other references:
http://secunia.com/advisories/16092/
http://www.kb.cert.org/vuls/id/150332
http://www.kb.cert.org/vuls/id/545804
http://www.kb.cert.org/vuls/id/870172
http://www.kb.cert.org/vuls/id/871756
http://www.kb.cert.org/vuls/id/891644
http://www.kb.cert.org/vuls/id/983340
http://www.kb.cert.org/vuls/id/999268

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

CVE Reference: None

❖ 13351 Oracle Database Server - TDE Wallet component Unspecified error (jan-2006/DB27)

An unspecified error in the TDE Wallet component can potentially be exploited to gain knowledge of certain information, overwrite arbitrary files, and to conduct SQL injection attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html
http://www.red-database-security.com/advisory/oracle_tde_wallet_password.html
http://www.red-database-security.com/advisory/oracle_tde_unencrypted_sga.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft_int.html
http://www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
http://www.red-database-security.com/advisory/oracle_reports_read_any_xml_file.html
http://www.imperva.com/application_defense_center/papers/oracle-dbms-01172006.html

Other references:
http://secunia.com/advisories/16092/
http://www.kb.cert.org/vuls/id/150332
http://www.kb.cert.org/vuls/id/545804
http://www.kb.cert.org/vuls/id/870172
http://www.kb.cert.org/vuls/id/871756
http://www.kb.cert.org/vuls/id/891644
http://www.kb.cert.org/vuls/id/983340
http://www.kb.cert.org/vuls/id/999268

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

CVE Reference: None

❖ 13352 Oracle Database Server - Upgrade & Downgrade component Unspecified error (jan-2006/DB28)

An unspecified error in the Upgrade & Downgrade component can potentially be exploited to gain knowledge of certain information, overwrite arbitrary files, and to conduct SQL injection attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html
http://www.red-database-security.com/advisory/oracle_tde_wallet_password.html
http://www.red-database-security.com/advisory/oracle_tde_unencrypted_sga.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft_int.html
http://www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
http://www.red-database-security.com/advisory/oracle_reports_read_any_xml_file.html
http://www.imperva.com/application_defense_center/papers/oracle-dbms-01172006.html

Other references:
http://secunia.com/advisories/16092/
http://www.kb.cert.org/vuls/id/150332
http://www.kb.cert.org/vuls/id/545804
http://www.kb.cert.org/vuls/id/870172
http://www.kb.cert.org/vuls/id/871756
http://www.kb.cert.org/vuls/id/891644
http://www.kb.cert.org/vuls/id/983340
http://www.kb.cert.org/vuls/id/999268

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

CVE Reference: None

New Vulnerabilities found this Week

Sun Java JRE "reflection" APIs Sandbox Security Bypass Vulnerabilities
"Read and write local files or execute local applications"

Seven vulnerabilities have been reported in Sun Java JRE (Java Runtime Environment), which potentially can be exploited by malicious people to compromise a user's system.

The vulnerabilities are caused due to various unspecified errors in the "reflection" APIs. This may be exploited by a malicious, untrusted applet to read and write local files or execute local applications.

The following releases are affected by one or more of the seven vulnerabilities on Windows, Solaris, and Linux platforms:
* JDK and JRE 5.0 Update 5 and prior
* SDK and JRE 1.4.2_09 and prior
* SDK and JRE 1.3.1_16 and prior

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102171-1

Sun Java System Directory Server LDAP Denial of Service
"Denial of Service"

Evgeny Legerov has discovered a vulnerability in Sun Java System Directory Server, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the LDAP server within the handling of certain requests. This can be exploited to crash the service via a specially-crafted request sent to the LDAP server port.

The vulnerability has been confirmed in version 5.2 P4. Other versions may also be affected.

References:
http://lists.immunitysec.com/pipermail/dailydave/2006-February/002914.html

PAM-MySQL SQL Logging and Authentication Vulnerabilities
"Denial of Service"

Some vulnerabilities have been reported in PAM-MySQL, which potentially can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system.

1) An unspecified error in the SQL logging facility can potentially be exploited to cause a DoS.

2) A double-free error exists in the authentication and authentication token alteration code when handling a pointer returned by the "pam_get_item()" function. This can be exploited by supplying a specially crafted password, which results in a DoS or can potentially be exploited to execute arbitrary code.

The vulnerabilities have been reported in versions 0.6.1 and 0.7pre2. Prior versions may also be affected.

References:
http://pam-mysql.sourceforge.net/News/00005.php
http://sourceforge.net/forum/forum.php?forum_id=499394
http://jvn.jp/cert/JVNVU%23693909/index.html
http://www.kb.cert.org/vuls/id/693909

Windows Insecure Service Permissions Privilege Escalation
"Gain escalated privileges"

Sudhakar Govindavajhala and Andrew W. Appel have reported some security issues in Microsoft Windows, which can be exploited by malicious, local users to gain escalated privileges.

Insecure SERVICE_CHANGE_CONFIG permissions on the UPnP, NetBT, SCardSvr, and SSDP services can be exploited to gain escalated privileges by changing the

associated program set to run by an identified service.

Successful exploitation allows an arbitrary program to be executed when an affected service is restarted.

The security issues have been reported in Windows XP SP1 (all listed services) and Windows Server 2003 (NetBT service).

References:
http://www.microsoft.com/technet/security/advisory/914457.mspx
http://www.cs.princeton.edu/~sudhakar/papers/winval.pdf
http://www.kb.cert.org/vuls/id/953860

Microsoft HTML Help Workshop ".hhp" Parsing Buffer Overflow
"Stack-based buffer overflow"

bratax has discovered a vulnerability in Microsoft HTML Help Workshop, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error within the handling of a ".hhp" file that contains an overly long string in the "Contents file" field. This can be exploited to cause a stack-based buffer overflow and allows arbitrary code execution when a malicious ".hhp" file is opened.

Note: An exploit is publicly available.

The vulnerability has been confirmed in version 4.74.8702.0. Other versions may also be affected.

References:
http://users.pandora.be/bratax/advisories/b008.html

Mozilla Suite XML Injection and Code Execution Vulnerabilities
"Conduct cross-site scripting attacks"

Two vulnerabilities have been reported in Mozilla Suite, which can be exploited by malicious people to conduct cross-site scripting attacks and potentially compromise a user's system.

References:
http://secunia.com/advisories/18703/

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