netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 42

October 20, 2006

Table of Contents

Product Focus

netVigilance will be attending Infosecurity 2006 in New York;scou where we will talk about vulnerability assessment, show you how a hacker works, show you our products. Come by booth 328. For details, visit http://www.netvigilance.com/events .

RPC DCOM Vulnerabilities Scanner – The RPC DCOM Vulnerabilities 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 Windows RPC DCOM flaws (MS03-026 and MS03-039).

This Week in Review

SQl injection not the only type. Removal of blacklist bad for businesses. Possible ICANN crisis. How to fight phishing.

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

- **Malicious code injection: It's not just about SQL anymore**

The good news: Developers are becoming increasingly aware of the threat posed by SQL injection attacks and the pitfalls of leaving pre vulnerable to such attacks. The bad

news: there are other types of pre injection attack, including LDAP injection and XPath injection, that can be just as dangerous to your applications and your data. While these may not be as well-known to developers as SQL injection, they are already in the hands of hackers, and they should be of concern. To make matters worse, much of the common wisdom concerning remediation of malicious pre injection attacks is inadequate or inaccurate.
The basic premise of all pre injection types

Hackers have many motives: They may wish to access a website or database that was intended only for a certain set of users. They may wish to access a database in order to steal such sensitive information as social security numbers and credit cards. They may wish to tamper with a database -- lowering prices, for example, so they can steal items from an e-commerce site with ease. And once an attacker has gained access to a database by using malicious pre, he may even be able to delete it completely, causing chaos for the business that has been attacked.

Security.itworld.com

Full Story :
http://security.itworld.com/4340/061019injection/page_1.html

- **Businesses will be hardest hit by removal of blacklists**

Australian businesses can expect a massive increase in spam if a US court carries out its threat to shut down the Spamhaus Project which is a non-profit, volunteer-run organization that compiles up-to-date blacklists of known spammers.

Internet Service Providers (ISPs) across the globe rely on the Spamhaus Project, which claims it blocks up to 50 billion spam e-mails per day.

Judge Charles Kocoras of the US District Court for the Northern District of Illinois threatened to shut down Spamhaus earlier this month for ignoring a $US11.7 million judgement against it for listing an e-mail company called E360Insight in its database of known spammers.

Spamhaus, based in London, has said that it ignored the judgement because it cannot be enforced in the UK.

Peter Stewart, A/NZ managing director of security e-mail provider TotalBlock, fears the court order will set a precedent for the closure of other blacklist organisations and without their protection global business communications could be severely disrupted.

"Blacklisting was never an efficient way of curbing spam, since far too many innocent e-mail users are wrongly listed and find it very difficult indeed to clear their names from blacklists," he said.

"Legal action against such lists was always on the cards, instigated either by legitimate e-mail users or spammers."

Computerworld

Full Story :
http://www.computerworld.com.au/index.php/id;1333132112;fp;4194304;fpid;1

❖ Spamhaus case could cause ICANN crisis

Internet experts are worried that a court decision against antispam blacklister The Spamhaus Project Ltd. could trigger a "constitutional crisis" for the Internet.

Last month, the District Court for the Northern District of Illinois ruled against the antispam project in a lawsuit brought by e-mail marketer e360Insight LLC. The court ordered Spamhaus to remove the company from its database of spammers and to pay $11.7 million in damages, but Spamhaus initially ignored the ruling, saying that the U.S. court had no jurisdiction over the U.K.-based project.

On Friday, the judge in the case upped the stakes. He issued a proposed order (download PDF) that told both the Spamhaus.org domain name registrar, Tucows Inc., and the Internet Corporation for Assigned Names and Numbers (ICANN) to pull the project's domain name, a move that would shut down the Spamhaus Web site.

Though the order is only proposed and does not have the force of law, observers said they worry that any attempt by U.S. courts to exert control over ICANN could be bad for the Internet.

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9004111&taxonomyId=17&intsrc=kc_feat

❖ Legislators Looking for Way to Fight Phishing

Phishing, the e-mail scam that keeps growing, is turning out to be a complex problem for the Utah Legislature. In fact, several lawmakers today admitted they're not sure how to deal with it.

It starts with an email that looks real. It could be from a bank, eBay, your credit union, or most recently MySpace. But the site doesn't have anything to do with those familiar businesses. For one thing, the email usually encourages you to click on a link that the legitimate site doesn't have. If you do link to it, the web address is long and complex, and again has nothing to do with the legitimate site.

The site will try to get you to enter personal information: account or credit card number, password, even social security number. What happens next could be inconvenient or it could lead to financial ruin.

Utah Legislation passed this year to crack down on phishing hasn't resulted in one conviction so far.

Kls.com

Full Story :
http://www.ksl.com/?nid=148&sid=578977#

New Vulnerabilities Tested in SecureScout

- **13437 Oracle Database Server - XMLDB component SQL Injection Vulnerability (oct-2006/DB01)**

An SQL Injection exists in ENABLE_HIERARCHY. The flaw actually lies in the ENABLE_HIERARCHY_INTERNAL procedure of the DBMS_XDBZ0 package. As XDB is not in the exclusion list for Oracle Application Server this flaw could be exploited without a user ID and password via the PLSQL Gateway.

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

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:

- **13438 Oracle Database Server - Oracle Spatial component SQL Injection Vulnerability (oct-2006/DB02)**

An SQL Injection exists in Trigger – into an anonymous PL/SQL block. The trigger fires when a user issues the
DROP USER statement. As the trigger is set to fire "before", it fires before the system checks to make
sure the user has the DROP USER privilege and is thus exploitable by anyone.

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

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:

❖ 13439 Oracle Database Server - Oracle Spatial component Buffer Overflow Vulnerability (oct-2006/DB03)

A Buffer overflow vulnerability exists in RELATE function
(calls MDIREL C function) SQL Injection in TESSELATE_FIXED
and TESSELATE. As MDSYS is not in the exclusion list for Oracle Application Server this flaw could be exploited without a user ID and password via the PLSQL Gateway.

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

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:

CVE Reference:

❖ 13440 Oracle Database Server - Change Data Capture (CDC) component SQL Injection Vulnerability (oct-2006/DB04)

An SQL Injection vulnerability exists in BUMP_SEQUENCE.
Also IMPORT_CHANGE_SET and IMPORT_SUBSCRIBER now call
DBMS_ASSERT.SIMPLE_SQL_NAME

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_cdc_impdp2.html

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

CVE Reference:

❖ 13441 Oracle Database Server - Change Data Capture (CDC) component SQL Injection Vulnerability (oct-2006/DB05)

An SQL Injection vulnerability exists in CREATE_CHANGE_TABLE – fixed "changeSourceType" in ChangeTable.class SQL Injection in CHANGE_TABLE_TRIGGER – fixed "fire" in ChangeTableTrigger.class CDC_DROP_CTABLE_BEFORE trigger is also an attack vector.

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:

❖ 13442 Oracle Database Server - Change Data Capture (CDC) component SQL Injection Vulnerability (oct-2006/DB06)

An SQL Injection vulnerability exists in PREPARE_UNBOUNDED_VIEW – fixed checkSubscribe in ChangeView.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:

❖ 13443 Oracle Database Server - Change Data Capture (CDC) component SQL Injection Vulnerability (oct-2006/DB07)

An SQL Injection vulnerability exists in CREATE_SUBSCRIPTION – fixed createSubscription in SubscriptionHandle.class and changeSetAdvEnabled in SubscriptionHandle.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:

❖ 13444 Oracle Database Server - Change Data Capture (CDC) component SQL Injection Vulnerability (oct-2006/DB08)

An SQL Injection vulnerability exists in EXTEND_WINDOW_LIST – fixed getChangeSetWindow in SubscriptionWindow.class. This can be exploited by creating a SET_NAME with embedded SQL. This flaw is fully discussed in the Oracle Hacker's Handbook.

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:

❖ 13445 Oracle Database Server - Core RDBMS component unknown Vulnerability (oct-2006/DB09)

An unknown vulnerability exists in Oracle Core RDBMS 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
http://www.red-database-security.com/advisory/oracle_modify_data_via_inline_views.html

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

CVE Reference:

❖ 13446 Oracle Database Server - Core RDBMS component SQL Injection Vulnerability (oct-2006/DB10)

An SQL Injection vulnerability exists in DROP_SQLSET, DELETE_SQLSET and SELECT_SQLSET.

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_sqltune_internal.html

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

CVE Reference:

❖ 13447 Oracle Database Server - Oracle Spatial component Length Check Vulnerability (oct-2006/DB11)

A Length checking vulnerability exists in RELATE function – then calls MD2.RELATE (see DB03 and DB22). As MDSYS is not in the exclusion list for Oracle Application Server this

flaw could be exploited without a user ID and password via the PLSQL Gateway.

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:

New Vulnerabilities found this Week

Opera Web Browser URL Handling Buffer Overflow Vulnerability

"Execution of arbitrary code"

A vulnerability has been reported in Opera Web Browser, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error when processing overly long URLs. This can be exploited to cause a heap-based buffer overflow by passing an overly long URL (more than 256 bytes) in a tag.

Successful exploitation allows execution of arbitrary code when a user visits a malicious website.

The vulnerability is reported in versions 9.0 and 9.01 on Windows and Linux. Version 8.x is reportedly not affected.

References:
http://www.opera.com/support/search/supsearch.dml?index=848
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=424

Internet Explorer 7 "mhtml:" Redirection Information Disclosure

"Information Disclose"

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/19738/

Oracle Products Multiple Vulnerabilities
"Denial of Service; conduct 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 cause a DoS (Denial of Service), conduct SQL injection attacks, and potentially compromise the system.

Details are available for the following vulnerabilities:

1) Various input processed by the following packages is not properly sanitized before being used in SQL queries. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code:
* DBMS_XDBZ
* SDO_DROP_USER_BEFORE
* MD2
* DBMS_CDC_IMPDP
* DBMS_CDC_IPUBLISH
* DBMS_CDC_ISUBSCRIBE
* DBMS_SQLTUNE
* SDO_GEOR_INT
* XDB_PITRIG_PKG
* SDO_DROP_USER
* SDO_CS

2) Boundary errors in the RELATE functions of the MD2 and SDO_GEOM packages, the GEOM_OPERATION function of the SDO_3GL package, and the TRANSFORM_LAYER function of the SDO_CS package may be exploited to cause a buffer overflow.

References:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html
http://descriptions.securescout.com/tc/13437
http://descriptions.securescout.com/tc/13438
http://descriptions.securescout.com/tc/13439
http://descriptions.securescout.com/tc/13440
http://descriptions.securescout.com/tc/13441
http://descriptions.securescout.com/tc/13442
http://descriptions.securescout.com/tc/13443
http://descriptions.securescout.com/tc/13444
http://descriptions.securescout.com/tc/13445
http://descriptions.securescout.com/tc/13446
http://descriptions.securescout.com/tc/13447

Apache HTTP Server mod_tcl Format String Vulnerabilities
"Execution of arbitrary code"

Some vulnerabilities have been reported in the mod_tcl module for Apache HTTP server, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerabilities are caused due to format string errors in tcl_cmds.c and tcl_core.c when calling the "set_var()" function with user-supplied input. This can be exploited by sending a specially crafted request containing format specifiers.

Successful exploitation allows execution of arbitrary code, but requires knowledge of the location of a tcl server script configured to use the vulnerable module for processing.

References:
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=421

Bugzilla Multiple Vulnerabilities
"Information Disclosure; conduct cross-site scripting, script insertion, and request forgery attacks"

Some vulnerabilities have been reported in Bugzilla, which can be exploited by malicious people or malicious users to disclose potentially sensitive information, conduct cross-site scripting, script insertion, and request forgery attacks.

1) Input passed to various fields and when embedded in <h1> and <h2> tags is not properly sanitized before being returned to users. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

2) An error when viewing attachments in "diff" mode allows users, who are not members of "insidergroup", to read the descriptions of all attachments. Additionally, when exporting bugs to the XML format, the "deadline" field is also visible for users, who are not member of the "timetrackinggroup" group. This can be exploited to gain knowledge of potentially sensitive information.

3) Bugzilla allows users to perform certain sensitive actions via HTTP GET and POST requests without verifying the user's request properly. This can be exploited to modify, delete, or create bugs.

4) Input passed to showdependencygraph.cgi is not properly sanitised before being returned to users. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

References:
http://www.bugzilla.org/security/2.18.5/

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