netVigilance

ScoutNews Team

October 21, 2005
Issue # 42

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

A bit of a slow new week for us - Snort gets hacked for looking back, smaller companies take the malware hit and ala Mytob; hackers quietly pinpoint revenue opportunities.

Stay safe out there

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

Top Security News Stories this Week

- **Snort vulnerability poses substantial risk**

A vulnerability in the popular freeware intrusion detection application; Snort could result in a worm attack that rivals SQL Slammer.

The real threat is due to the fact that many corporations may be running Snort without realizing it. Snort is somewhat innocuously embedded in many third-party IDS appliances.

The vulnerability is contained within a preprocessor used to detect an essentially obsolete Trojan called Back Orifice.

Related Links :

http://www.us-cert.gov/cas/techalerts/TA05-291A.html http://www.crn.com/sections/security/security.jhtml?articleId=172302520

http://www.securityfocus.com/news/11349?ref=rss

- **Smaller companies get hit with Malware more often**

In a report issued by Tokyo based Trend Micro; smaller firms tend to get brunt of malware attacks. Smaller companies that are often strapped for IT resources are seeing more disruption of business that larger; better funded companies.

Did someone say vulnerability assessment? – *Ed.*
CIOL

Full Story:
http://www.ciol.com/content/news/2005/105102005.asp

- **Virus attacks rise – as rifle shots vs. shotgun**

Sophos reports a continued increase in the number of detected Viruses this year. Motivated by profit as opposed to notoriety; virus authors are creating malware that takes direct aim at specific organizations.

This new generation of viruses and worms seek to steal user's information before they can be detected or before awareness can be raised in the media.

The 2 anti-virus / anti-spyware vendors contributing to this story; Sophos and Central Command offer completely differing data on the top five most prevalent threats, although Mytob variants seem to be pervasive.
eSecurityPlanet.com

Full Story:
http://www.esecurityplanet.com/trends/article.php/3554046

Related Links:
http://www.internetnews.com/security/article.php/3557611

New Vulnerabilities Tested in SecureScout

- **13289 Oracle Database Server - PL/SQL component Unspecified error (oct-2005/DB01)**

An unspecified error in the PL/SQL component can potentially be exploited to disclose or manipulate information.

A buffer overflow vulnerability and seventeen PL/SQL injection vulnerabilities exists in Oracle Database 10g and Oracle9i Database Server.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

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

CVE Reference: CAN-2005-0873

❖ 13290 Oracle Database Server - Change Data Capture component Unspecified error (oct-2005/DB02)

An unspecified error in the Change Data Capture component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

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

CVE Reference: CAN-2005-0873

❖ 13291 Oracle Database Server - Change Data Capture component Unspecified error (oct-2005/DB03)

An unspecified error in the Change Data Capture component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

Product Homepage:

http://www.oracle.com/

CVE Reference: CAN-2005-0873

❖ 13292 Oracle Database Server - Change Data Capture component Unspecified error (oct-2005/DB04)

An unspecified error in the Change Data Capture component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

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

CVE Reference: CAN-2005-0873

❖ 13293 Oracle Database Server - Change Data Capture component Unspecified error (oct-2005/DB05)

An unspecified error in the Change Data Capture component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

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

CVE Reference: CAN-2005-0873

❖ 13294 Oracle Database Server - Data Guard Logical Standby component Unspecified error (oct-2005/DB06)

An unspecified error in the Data Guard Logical Standby component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

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

CVE Reference: CAN-2005-0873

❖ 13295 Oracle Database Server - Data Pump Export component Unspecified error (oct-2005/DB07)

An unspecified error in the Data Pump Export component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

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

CVE Reference: CAN-2005-0873

❖ 13296 Oracle Database Server - Database Scheduler component Unspecified error (oct-2005/DB08)

An unspecified error in the Database Scheduler component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

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

CVE Reference: CAN-2005-087

- ❖ **13297 Oracle Database Server - Export component Unspecified error (oct-2005/DB09)**

An unspecified error in the Export component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

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

CVE Reference: CAN-2005-0873

- ❖ **13298 Oracle Database Server - Locale component Unspecified error (oct-2005/DB10)**

An unspecified error in the Locale component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

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

CVE Reference: CAN-2005-0873

New Vulnerabilities found this Week

- ❖ **Oracle Products 85 Unspecified Vulnerabilities**
  "Conduct PL/SQL injection attacks, cross-site scripting attacks, or potentially to compromise a vulnerable system."

  85 vulnerabilities have been reported in various Oracle products. Some have an unknown impact, and others can be exploited to conduct PL/SQL injection attacks, cross-site scripting attacks, or potentially to

compromise a vulnerable system.

Details have been disclosed for the following vulnerabilities:

1) A buffer overflow vulnerability and seventeen PL/SQL injection vulnerabilities exists in Oracle Database 10g and Oracle9i Database Server.

2) Some input passed to "test.jsp" of the Oracle Reports Server isn't properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

3) Some Oracle Applications database accounts have excessive system privileges assigned, and some default application accounts are enabled and have default passwords.

4) Input passed to the "end date" field in "wf_route.CreateRule", and to the "response form" field in "wf_monitor.find_instance", isn't properly sanitized before being returned to the Oracle Workflow user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in the context of an affected site.

References:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html
http://www.integrigy.com/alerts/OraCPU1005.htm
http://www.red-database-security.com/advisory/oracle_workflow_css_wf_route.html
http://www.red-database-security.com/advisory/oracle_workflow_css_wf_monitor.html
http://www.kb.cert.org/vuls/id/210524

❖ **Snort Back Orifice Pre-Processor Buffer Overflow Vulnerability**
"Boundary error"

Neel Mehta has reported a vulnerability in Snort, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the handling of Back Orifice packets. This can be exploited by sending a maliciously crafted UDP packet to a network or device protected by or running an IDS or IPS system based on Snort.

The vulnerability has been reported in Snort version 2.4.0 , 2.4.1, and 2.4.2. Other versions may also be affected.

References:
http://www.snort.org/pub-bin/snortnews.cgi#99

http://xforce.iss.net/xforce/alerts/id/207
http://www.kb.cert.org/vuls/id/175500

- ### Cisco CSS SSL Client Certificate Handling Denial of Service

"Denial of Service"

A vulnerability has been reported in Cisco 11500 CSS (Content Services Switch), which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to a memory corruption error when processing malformed client certificate during SSL session negotiation. This can be exploited to cause the CSS to reload via a specially crafted client certificate even when the CSS did not request for a client certificate during SSL session negotiation.

Successful exploitation requires that CSS is configured to provide SSL termination services.

The vulnerability has been reported in 11500 Series CSS running version 7.1 through 7.5 of the Cisco WebNS operating system.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20051019-css.shtml

- ### Squid FTP Server Response Handling Denial of Service

"Denial of Service"

M.A.Young has reported a vulnerability in Squid, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in handling certain FTP server responses. This can be exploited to crash Squid by visiting a malicious FTP server via the proxy.

The vulnerability has been reported in Squid-2.5 and prior.

References:
http://www.squid-cache.org/Versions/v2/2.5/bugs/#squid-2.5.STABLE11-rfc1738_do_escape

- ### Network Security Services (NSS) Library Zlib Vulnerability

"Denial of Service"

A vulnerability has been reported in Network Security Services (NSS), which potentially can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system.

The vulnerability is caused due to the use of a vulnerable version of zlib.

For more information:
SA15949

The vulnerability affects version 3.10. Prior versions may also be affected. NSS tools such as "signtool" and "modutil" are also affected.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101989-1
http://secunia.com/advisories/15949/

- **Linux Kernel Console Keyboard Mapping Shell Command Injection**
  "Gain escalated privileges"

  Rudolf Polzer has reported a vulnerability in the Linux Kernel, which potentially can be exploited by malicious, local users to gain escalated privileges.

  The vulnerability is caused due to the way console keyboard mapping is handled. The keyboard map installed by a local user using "loadkeys" is applied to all virtual consoles and is not being reset after the user logs out.

  Successful exploitation allows malicious console users to inject arbitrary shell commands into certain key mappings, which are executed when the next logon console user uses the re-mapped key.

  The vulnerability has been reported in Kernel 2.6. Other versions may also be affected.

  References:
  http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=334113

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