netVigilance

ScoutNews Team

January 27, 2006
2006 Issue # 4

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review
Top Security News Stories this Week
New Test Cases Tested in SecureScout
New Vulnerabilities this Week

This Week in Review

Linux / Unix holier than Windows, ChoicePoint marks historical settlement with Feds over data loss, Maleware: Frequency down – Damage up, Chinese hackers fail to break into Parliament and Roger Grimes of InfoWorld gives us a VISTA security picture.

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

❖ Unix / Linux leads Windows on vulnerability count

In it's year-end vulnerability summary; US-CERT states that Unix / Linux OSs contained 3 times as many vulnerabilities than Windows. The CERT numbers for 2005: Linux / Unix = 2,328, Windows = 812.

Full Story:
http://www.varbusiness.com/showArticle.jhtml?articleId=175801167

❖ ChoicePoint to pay $15M in penalties for loss of data

ChoicePoint has agreed to a 15 Million dollar settlement with the FTC as a result of loosing personal financial information on 160,000 credit card customers in February of 2005. This represents the largest settlement in the history of the FTC.

RedHerring

Full Story : http://www.redherring.com/Article.aspx?a=15484&hed=ChoicePoint+Settles+with+FTC&sector=Industries&subsector=SecurityAndDefense

❖ Malware numbers down, Severity up

Although the number of reported malware attacks was down significantly last year; the severity of these types of attacks has greatly increased. The data from IBM's latest Global Business Security Index; reports that attacks are often directed at government departments or military installations with the intent of stealing data, stealing identities, and selling botnets.

The Register

Full Story :

http://www.theregister.co.uk/2006/01/25/ibm_cybercrime_report_2005/

❖ Brits repel Chinese attacks on Parliament

A January 2nd attack launched from servers in China's Guangdong Province; attempted to exploit the Windows Meta File (WMF) vulnerability to hijack more than 70 PCs. Emails were sent to staff, with an attachment that contained the WMF-exploiting Setabortproc Trojan. Since this attack specifically named individuals; it is suspected that it was part of a more general campaign of electronic espionage.

TechWorld

Full Story :

http://www.techworld.com/security/news/index.cfm?NewsID=5235&inkc=0

❖ A preview of Microsoft VISTA security features

User Account Control, Integrated AntiSpyware, Secure Startup and improved auditing are just some of the advanced security features included in the VISTA release. It's worth the read to understand how this will affect your world as a Windows administrator.

InfoWorld

Related Links : http://www.infoworld.com/article/06/01/27/74782_05OPsecadvise_1.html

New Vulnerabilities Tested in SecureScout

❖ 13325 Oracle Database Server - Advanced Queuing component Unspecified error (jan-2006/DB01)

An unspecified error in the Advanced Queuing 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

❖ 13326 Oracle Database Server - Change Data Capture component Unspecified error (jan-2006/DB02)

An unspecified error in the Change Data 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

❖ 13327 Oracle Database Server - Connection Manager component Unspecified error (jan-2006/DB03)

An unspecified error in the Connection Manager 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

❖ 13328 Oracle Database Server - Data Pump component Unspecified error (jan-2006/DB04)

An unspecified error in the Data Pump 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

❖ 13329 Oracle Database Server - Data Pump Metadata API component Unspecified error (jan-2006/DB05) 13330 Oracle Database Server - Data Pump Metadata API component Unspecified error (jan-2006/DB06)

An unspecified error in the Data Pump Metadata API 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

❖ 13331 Oracle Database Server - Dictionary component Unspecified error (jan-2006/DB07)

An unspecified error in the Data Pump Metadata API 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

❖ 13332 Oracle Database Server - Net Foundation Layer component Unspecified error (jan-2006/DB08)

An unspecified error in the Net Foundation Layer 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

❖ 16098 Linux Kernel error in the "mmap()" function to be exploited to cause a DoS or potentially gain escalated privileges

A vulnerability has been reported in the Linux kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service) or potentially gain escalated privileges.

An error in the "mmap()" function may result in creation of memory maps with a start address after the end address. This can be exploited to cause a DoS or potentially gain escalated privileges.

The vulnerability has been fixed in version 2.6.11.11.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11.11
http://www.ubuntulinux.org/support/documentation/usn/usn-137-1

Other references:
http://secunia.com/advisories/15630/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-0756, CAN-2005-1265

❖ 16099 Linux Kernel pktcdvd and raw device Block Device Vulnerabilities

alert7 has reported two vulnerabilities in the Linux kernel, which can be exploited by malicious, local users to gain escalated privileges.

Input validation errors in the raw device and pktcdvd block device ioctl handlers (raw_ioctl() and pkt_ioctl() functions) can be exploited to corrupt kernel memory via specially crafted arguments passed to the ioctl_by_bdev() function.

Successful exploitation allows execution of arbitrary code with kernel level privileges, but requires that the user can read the affected block device.

The vulnerability has been fixed in version 2.6.11.10.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11.10

Other references:
http://secunia.com/advisories/15392/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-1264, CAN-2005-1589

New Vulnerabilities found this Week

nfs-server "rpc.mountd" Buffer Overflow Vulnerability
“Buffer overflow”

A vulnerability has been reported in nfs-server, which can be exploited by malicious users to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the "realpath()" function used by rpc.mountd. This can be exploited to cause a buffer overflow when processing mount requests.

Successful exploitation allows arbitrary code execution with root privileges but requires the ability to create symlinks on any of the file systems on the machine running rpc.mountd. The vulnerability may also be exploitable by users without filesystem access.

References:
http://lists.suse.com/archive/suse-security-announce/2006-Jan/0007.html

Sun StorEdge Enterprise Backup / Solstice Backup Vulnerabilities

“Denial of Service”

Sun has acknowledged some vulnerabilities in Sun StorEdge Enterprise Backup and Solstice Backup, which can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system.

The vulnerabilities have been reported in the following products:
* Sun StorEdge Enterprise Backup versions 7.0, 7.1, and 7.2.
* Solstice Backup versions 6.0 and 6.1.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102148-1

Cisco IOS AAA Command Authentication Bypass Vulnerability
“Bypass certain security restrictions”

A vulnerability has been reported in Cisco IOS, which can be exploited by malicious, local users to bypass certain security restrictions.

The vulnerability is caused due to missing authorisation checks in the AAA (Authentication, Authorization, and Accounting) command authorisation feature for commands that are executed from the Tcl (Tool Command Language) exec shell. This can be exploited by malicious users to execute any IOS EXEC command at the users' authenticated privilege level.

Successful exploitation requires that the AAA command authorisation feature is enabled and Tcl functionality is supported by the device.

The vulnerability has been reported in IOS Version 12.0T or later.

Note: It has also been reported that an authenticated user is automatically placed into the Tcl Shell mode if a previous user goes into Tcl Shell mode and terminates the session before leaving the Tcl Shell mode. This may help to exacerbate the vulnerability.

References:
http://www.cisco.com/warp/public/707/cisco-response-20060125-aaatcl.shtml

Mercury Mail Transport System Buffer Overflow
“Buffer overflow”

kcope has discovered a vulnerability in Mercury Mail Transport System, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the request handling in the "MercuryH PH Directory Server" protocol module. This can be exploited to cause a buffer overflow by sending overly long data to port 105/tcp.

Successful exploitation allows execution of arbitrary code.

NOTE: Exploit code is publicly available.

The vulnerability has been confirmed in version 4.01b. Other versions may also be affected.

References:
http://secunia.com/advisories/18611/

Red Hat Directory Server / Certificate Server Buffer Overflow

"Gain root privileges"

Peter Winter-Smith of NGSSoftware has reported a vulnerability in Red Hat Directory Server and Red Hat Certificate System, which can be exploited by malicious, local users to gain escalated privileges and potentially by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error related to the Help buttons available in the Admin pages of the Management Console. This can be exploited to cause a stack-based buffer overflow by connecting to the Management Console and sending a specially crafted request.

According to the vendor, it is not possible to exploit the vulnerability remotely on Unix systems. However, it is exploitable by local users to gain root privileges.

The vulnerability has been reported in Red Hat Directory Server 7.1, Red Hat Certificate
System 7.1, and prior Netscape releases of these products.

References:
http://secunia.com/advisories/18590/

OpenSSH scp Command Line Shell Command Injection

"Escalated privileges"

Josh Bressers has reported a weakness in OpenSSH, which potentially can be exploited by malicious, local users to perform certain actions with escalated privileges.

The weakness is caused due to the insecure use of the "system()" function in scp when performing copy operations using filenames that are supplied by the user from the command line. This can be exploited to execute shell commands with privileges of the user running scp.

Successful exploitation requires that the user is e.g. tricked into using scp to copy a file with a specially crafted filename.

The weakness has been confirmed in version 4.2p1. Other versions may also be affected.

References:
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174026

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