netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 16

April 21, 2006

Table of Contents

Product Focus - Messenger Service Vulnerability Scanner free single vulnerability scanner. Examine up to 256 unique IP addresses for vulnerabilities that exist in Microsoft's messenger service.

This Week in Review

SenderID gaining steam for fighting Spam and Phishers, War on hackers at a stalemate, companies spending more to fight cyber crime and Linux living with OSX and XP on Macs.

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

- **SenderID gains favor to fight Spam, Phishing**

Microsoft seems serious about throwing its weight behind the SenderID framework for authentication of email messages. Sender ID seeks to verify that every e-mail message originates from the Internet domain from which it claims to have been sent. This is accomplished by checking the address of the server sending the mail against a registered list of servers that the domain owner has authorized to send e-mail.

The system relies on adoption by companies to generate SenderID-compliant emails. Apparently, this is happening, with morethan 3.3 Million domains worldwide participating.
eCommerce Times

Full Story :
http://www.ecommercetimes.com/rsstory/50040.html

❖ Security Professionals treading water

ZDNet UK has published a report on the state of the battle against hackers – currently at a stalemate. The report finds that IT professionals are still consumed with addressing security issues as opposed to building infrastructure to increase productivity. The full report is available for download from the site below.
ZDNet

Full Story:

http://news.zdnet.co.uk/business/0,39020645,39264028,00.htm

❖ Security expenditures increase on hacker news

Gartner finds that companies have shifted focus of IT spending toward protecting vital data. With stories of customer data losses dominating 2005 and making the nightly news; the awareness and cost have shot up.

Gartner puts the cost of data loss at $90 / record. With the amount of data being stored by even medium sized companies, the cost of getting hacked quickly impacts the bottom line. Take for example the case of CardSystems: the loss of 40 million credit card numbers has already cost them $1 Billion.
redHerring

Full Story :

http://www.redherring.com/Article.aspx?a=16544&hed=Data+Security+Spending+Rises&sector=Industries&subsector=SecurityAndDefense

❖ Hackers crack triple-boot of Mac – adding Linux to list

Following the release of the Boot Camp package by Apple, allowing iMac users to dualboot either OSX or XP; hackers published a method to vector to Linux as well.

The article goes on to explain how intrepid iMac owners can serve up a smorgasbord of OSs on their systems.

eWeek

Related Links:

http://www.eweek.com/article2/0,1895,1952037,00.asp
http://www.bit-tech.net/news/2006/04/20/linux_bootcamp_triple_boot/

New Vulnerabilities Tested in SecureScout

13354 Oracle Database Server - Advanced Replication component Arbitrary SQL Injection error (apr-2006/DB01)

An SQL injection vulnerability in the Oracle DBMS_REPUTIL package may allow a remote attacker to execute arbitrary SQL commands on a vulnerable Oracle installation

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2006.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2006.html
http://www.kb.cert.org/vuls/id/139049
http://www.us-cert.gov/cas/techalerts/TA06-109A.html
http://secunia.com/advisories/19712/

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

CVE Reference: None

13355 Oracle Database Server - Advanced Replication component SQL Injection issues (apr-2006/DB02)

An SQL injection vulnerability in one of the Oracle package may allow a remote attacker to execute arbitrary SQL commands on a vulnerable Oracle installation.

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

References:

Original Advisory:

http://www.oracle.com/technology/deploy/security/pdf/cpuapr2006.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2006.html
http://www.us-cert.gov/cas/techalerts/TA06-109A.html
http://secunia.com/advisories/19712/

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

CVE Reference: None

❖ 13356 Oracle Database Server - Advanced Replication component SQL Injection issues (apr-2006/DB03)

An SQL injection vulnerability in the Oracle Advanced Replication component may allow a remote attacker to execute arbitrary SQL commands on a vulnerable Oracle installation.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2006.html

Other references:
http://www.argeniss.com/research/ARGENISS-ADV-040603.txt
http://www.red-database-security.com/advisory/oracle_cpu_apr_2006.html
http://www.kb.cert.org/vuls/id/797465
http://www.us-cert.gov/cas/techalerts/TA06-109A.html
http://secunia.com/advisories/19712/

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

CVE Reference: None

❖ 13357 Oracle Database Server - Dictionary component unspecified vulnerability (apr-2006/DB04)

An unspecified vulnerability in the Oracle Dictionary component may allow a remote attacker to compromise system integrity and availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2006.html

Other references:

http://www.red-database-security.com/advisory/oracle_cpu_apr_2006.html
http://www.kb.cert.org/vuls/id/241481
http://www.us-cert.gov/cas/techalerts/TA06-109A.html
http://secunia.com/advisories/19712/

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

CVE Reference: None

❖ 13358 Oracle Database Server - Export component SQL injection vulnerability (apr-2006/DB05)

An SQL injection vulnerability in the Oracle Export component may allow a remote attacker to execute arbitrary SQL commands on a vulnerable Oracle installation.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2006.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2006.html
http://www.kb.cert.org/vuls/id/452681
http://www.us-cert.gov/cas/techalerts/TA06-109A.html
http://secunia.com/advisories/19712/

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

CVE Reference: None

❖ 13359 Oracle Database Server - Log Miner component SQL injection vulnerability (apr-2006/DB06)

An SQL injection vulnerability in the Oracle Log Miner component may allow a remote attacker to execute arbitrary SQL commands on a vulnerable Oracle installation.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2006.html

Other references:
http://www.red-database-security.com/advisory/oracle_sql_injection_dbms_logmnr_session.html
http://www.red-database-security.com/advisory/oracle_cpu_apr_2006.html
http://www.us-cert.gov/cas/techalerts/TA06-109A.html

http://secunia.com/advisories/19712/

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

CVE Reference: None

❖ 13360 Oracle Database Server - Oracle Enterprise Manager Intelligent Agent component unspecified vulnerability (apr-2006/DB07)

An unspecified vulnerability in the Oracle Enterprise Manager Intelligent Agent component may allow a remote attacker to compromise system integrity and availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2006.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2006.html
http://www.us-cert.gov/cas/techalerts/TA06-109A.html
http://secunia.com/advisories/19712/

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

CVE Reference: None

❖ 13361 Oracle Database Server - Oracle Spatial component unspecified vulnerability (apr-2006/DB08)

An unspecified vulnerability in the Oracle Spatial component may allow a remote attacker to compromise system integrity and availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2006.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2006.html
http://www.us-cert.gov/cas/techalerts/TA06-109A.html
http://secunia.com/advisories/19712/

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

CVE Reference: None

❖ 13362 Oracle Database Server - Oracle Spatial component SQL Injection vulnerability (apr-2006/DB09)

An SQL injection vulnerability in the Oracle Spatial component may allow a remote attacker to execute arbitrary SQL commands on a vulnerable Oracle installation.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2006.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2006.html
http://www.us-cert.gov/cas/techalerts/TA06-109A.html
http://secunia.com/advisories/19712/

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

CVE Reference: None

❖ 13363 Oracle Database Server - Oracle Spatial component SQL Injection vulnerability (apr-2006/DB10)

An SQL injection vulnerability in the Oracle Spatial component may allow a remote attacker to execute arbitrary SQL commands on a vulnerable Oracle installation.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2006.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2006.html
http://www.us-cert.gov/cas/techalerts/TA06-109A.html
http://secunia.com/advisories/19712/

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

CVE Reference: None

New Vulnerabilities found this Week

Cisco IOS XR MPLS Denial of Service Vulnerabilities

“Denial of Service”

Three vulnerabilities have been reported in Cisco IOS XR, which can be exploited by malicious people to cause a DoS (Denial of Service).

All three vulnerabilities are caused due to unspecified errors within the processing of MPLS (Multi Protocol Label Switching) packets. This can be exploited via specially crafted MPLS packets to restart the NetIO process, which causes a Modular Services Card on a Cisco Carrier Routing System 1 (CRS-1) or a Line Card on a Cisco 12000 series router to reload.

Successful exploitation requires that MPLS has been configured on the network device.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20060419-xr.shtml

Linux Kernel perfmon Local Denial of Service Vulnerability

“Denial of Service”

A vulnerability has been reported in Linux Kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in perfmon (perfmon.c) during exit processing and may cause a crash when a task is interrupted while another process is accessing the "mm_struct" structure.

References:
http://secunia.com/advisories/19737/

Linux Kernel x87 Register Information Leak

“Gain knowledge of potentially sensitive information”

A security issue has been reported in Linux Kernel, which can be exploited by malicious, local users to gain knowledge of potentially sensitive information.

The problem is caused due to AMD K7/K8 CPUs only saving/restoring certain x87 registers in FXSAVE instructions when an exception is pending. This may leak x87 register information between processes.

References:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.9

AWStats Cross-Site Scripting and Full Path Disclosure

“Disclose system information; conduct cross-site scripting attacks”

r0t has discovered some vulnerabilities in AWStats, which can be exploited by malicious people to disclose system information and conduct cross-site scripting attacks.

1) Some input isn't properly sanitised 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.

2) The problem is that it is possible to disclose the full path to the installation by supplying an invalid "config" parameter to "awstats.pl".

The vulnerabilities have been confirmed in version 6.5. Other versions may also be affected.

References:
http://pridels.blogspot.com/2006/04/awstats-65-vuln.html
http://pridels.blogspot.com/2006/04/awstats-65x-multiple-vuln.html

FreeBSD FPU x87 Register Information Leak
"Gain knowledge of potentially sensitive information"

A security issue has been reported in FreeBSD, which can be exploited by malicious, local users to gain knowledge of potentially sensitive information.

The problem is caused due to AMD K7/K8 CPUs only saving/restoring certain x87 registers in FXSAVE instructions when an exception is pending. This may leak x87 register information between processes.

References:
ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-06:14.fpu.asc
ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-06:14-amd.txt

Oracle Products Multiple Vulnerabilities
"Conduct SQL injection attacks; compromise a vulnerable system."

Multiple vulnerabilities have been reported in various Oracle products. Some have an unknown impact, and others can be exploited to conduct SQL injection attacks or compromise a vulnerable system.

References:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2006.html
http://descriptions.securescout.com/tc/13354
http://descriptions.securescout.com/tc/13355
http://descriptions.securescout.com/tc/13356
http://descriptions.securescout.com/tc/13357
http://descriptions.securescout.com/tc/13358
http://descriptions.securescout.com/tc/13359
http://descriptions.securescout.com/tc/13360
http://descriptions.securescout.com/tc/13361
http://descriptions.securescout.com/tc/13362
http://descriptions.securescout.com/tc/13363

Linux Kernel "ip_route_input()" Denial of Service Vulnerability
"Denial of Service"

A vulnerability has been reported in Linux Kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

The vulnerability is caused due to a NULL pointer dereference error in the "ip_route_input()" function when the route is requested for a multi-cast IP address.

References:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.8

Linux Kernel Shared Memory Restrictions Bypass

"Bypass certain security restrictions"

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

References:
http://secunia.com/advisories/19657/

Linux Kernel Shared Memory Restrictions Bypass

"Bypass certain security restrictions"

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

The vulnerability is caused due to the "mprotect()" function giving write permissions to read-only attachments of shared memory regardless of the permissions given by IPC.

References:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.6
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.7

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