netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 29

July 21, 2006

Table of Contents

Product Focus

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

Black hat 2006 announces exposure of 15 security vulnerabilities. Fed scientists to share knowledge with public. Time to start looking out for your VoIP. Customization weakest link.

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

- **Black Hat 2006 set to expose security flaws**

This month's Black Hat USA 2006 conference will again expose security vulnerabilities in some of the world's biggest network and IT suppliers' products.

Serious flaws are set to be demonstrated in various technologies by security researchers at the Las Vegas hacking gathering.

Around 15 new exploits are scheduled to be discussed, according to conference organisers.

Last year, Cisco issued a lawsuit against the organisers after one of its former employees demonstrated a serious security hole in its routing technology.

The two sides settled after the organisers agreed not to disseminate the information widely, even though details had already been spread over the internet.

This year, two new vulnerabilities in Network Admission Control (NAC) and voice over IP technologies will be demonstrated. They affect multiple suppliers, including Cisco.

As part of the proceedings, bugs will also be exposed in the Linux-based Asterisk PBX (private branch exchange) telephony software, as will three exploits in Oracle software and four in Microsoft programs. Other Linux exploits will also be discussed, as well as one related to products from Xerox.

Computerwekly

Full Story :
http://www.computerweekly.com/Articles/2006/07/20/217108/Black+Hat+2006+set+to+expose+security+flaws.htm

- **Scientists teaching power grid, dam operators how to thwart hackers Government to sponsor cybersecurity summit**

Federal scientists who study how hackers try to break into computer-based controls for water treatment plants, power grids, nuclear reactors and other automated industrial systems are passing the secrets on to private operators of such facilities at no charge.

The U.S. Department of Energy and U.S. Department of Homeland Security will sponsor classes in protecting remote controls of critical infrastructure from hackers during an international cybersecurity summit in Las Vegas Sept. 28-30.

The Associated Press

Full Story :
http://www.idahostatesman.com/apps/pbcs.dll/article?AID=/20060720/NEWS02/607200346/1029

- **Security Honeymoon Over For VoIP**

Last month's FBI arrest of a man in Miami for allegedly hacking into the networks of Internet service providers has ushered in a new era for voice over IP technology (VoIP).

Naturally, VoIP inevitably was going to have to deal with the same type of security concerns that other data networks have faced. But the security space moves fast, and in recent months VoIP security has gone from an impending issue to a top-of-mind problem for vendors, VARs and users.

Network Computing

Full Story :
http://www.networkcomputing.com/channels/security/showArticle.jhtml;jsessionid=NJNX

32VTXUY1KQSNDLOSKH0CJUNN2JVN?articleID=190700111

- **Weakest link in app security is customization**

The customization of off-the-shelf software is the weakest link in application security. This is particularly true for widely used enterprise products such as SAP and Oracle, according to Gartner research director Rich Mogull.

He said the massive amounts of customization required to get products from both SAP and Oracle to perform ideally means that IT managers have no failsafe point if some of the code creates vulnerabilities. As a result, managers have to cherrypick through code to find their own mistakes as opposed to downloading a patch from a vendor.

Speaking at the Gartner IT Security Summit in Sydney last week, Mogull said this problem has created custom vulnerabilities.

"Custom code does not undergo the same QA testing as commercial code does," Mogull said.

Computerworld

Full Story :
http://www.computerworld.com.au/index.php/id;65524373;fp;16;fpid;0

New Vulnerabilities Tested in SecureScout

- **13368 Microsoft SQL Server "sa" Password Vulnerability**

The remote MS SQL server has the default 'sa' account
enabled with password "sa".
An attacker may use this flaw to execute commands against the remote host, as well as read your database content.

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

References:

CERT Vulnerability Note: http://www.kb.cert.org/vuls/id/635463
BID: http://online.securityfocus.com/bid/4797
SANS Top 20 Microsoft SQL Server (MSSQL): http://www.sans.org/top20/#W2

CVE Reference: CAN-2000-1209

- **13369 Microsoft SQL Server Version Disclosure**

Identifying the remote Microsoft SQL Server version could be useful in further attacks against the target.

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

References:
SANS Top 20 Microsoft SQL Server (MSSQL): http://www.sans.org/top20/#W2

Home page:
http://www.microsoft.com/sql/default.mspx

CVE Reference:

❖ 13370 Oracle Database Server - Change Data Capture (CDC) component SQL Injection vulnerability (jul-2006/DB01)

An SQL Injection vulnerability in the Change Data Capture (CDC) component may allow a remote attacker to compromise system integrity and availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
BUGTRAQ:20060718 Oracle Database - SQL Injection in SYS.DBMS_CDC_IMPDP [DB01]
URL:http://www.securityfocus.com/archive/1/archive/1/440440/100/0/threaded
BUGTRAQ:20060718 Oracle Database - SQL Injection in SYS.KUPW$WORKER [DB03]
URL:http://www.securityfocus.com/archive/1/archive/1/440439/100/0/threaded
MISC: http://www.red-database-security.com/advisory/oracle_sql_injection_dbms_cdc_impdp.html
MISC: http://www.red-database-security.com/advisory/oracle_sql_injection_kupw$worker.html
CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
MISC: http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

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

CVE Reference: CVE-2006-3698

❖ 13371 Oracle Database Server - Core RDBMS component unspecified vulnerability (jul-2006/DB02)

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

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
CONFIRM: ttp://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
MISC: http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

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

CVE Reference: CVE-2006-3699

❖ 13372 Oracle Database Server - Data Pump Metadata API component SQL Injection vulnerability (jul-2006/DB03)

An SQL Injection vulnerability in the Data Pump Metadata API component may allow a remote attacker to compromise system integrity and availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
BUGTRAQ:20060718 Oracle Database - SQL Injection in SYS.DBMS_CDC_IMPDP [DB01]
URL:http://www.securityfocus.com/archive/1/archive/1/440440/100/0/threaded

BUGTRAQ:20060718 Oracle Database - SQL Injection in SYS.KUPW$WORKER [DB03]
URL:http://www.securityfocus.com/archive/1/archive/1/440439/100/0/threaded
MISC: http://www.red-database-security.com/advisory/oracle_sql_injection_dbms_cdc_impdp.html
MISC: http://www.red-database-security.com/advisory/oracle_sql_injection_kupw$worker.html
CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
MISC: http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

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

CVE Reference: CVE-2006-3699

❖ 13373 Oracle Database Server - Web Distributed Authoring and Versioning (DAV) component SQL Injection vulnerability (jul-2006/DB04)

An SQL Injection vulnerability in the Web Distributed Authoring and Versioning (DAV) component may allow a remote attacker to compromise system integrity and availability.

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

References:
Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
MISC: http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529

URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

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

CVE Reference: CVE-2006-3700

❖ 13374 Oracle Database Server - Dictionary component Buffer Overflow vulnerability (jul-2006/DB05)

A Buffer Overflow vulnerability in the Dictionary component may allow a remote attacker to compromise system integrity and availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
MISC: http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

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

CVE Reference: CVE-2006-3701

❖ 13375 Oracle Database Server - Export component SQL Injection vulnerability (jul-2006/DB06)

An SQL Injection vulnerability in the Export component may allow a remote attacker to compromise system integrity and availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
MISC: http://www.red-database-security.com/exploits/oracle-sql-injection-oracle-dbms_export_extension.html
CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
MISC: http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
CERT-VN:VU#932124
URL:http://www.kb.cert.org/vuls/id/932124
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

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

CVE Reference: CVE-2006-3702

❖ 13376 Oracle Database Server - InterMedia component Buffer Overflow vulnerability (jul-2006/DB07)

A Buffer Overflow vulnerability in the InterMedia component may allow a remote attacker to compromise system integrity and availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
MISC: http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863

SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

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

CVE Reference: CVE-2006-3703

❖ **13377 Oracle Database Server - OCI component Modify Data via Views vulnerability (jul-2006/DB08)**

A Modify Data via Views vulnerability in the OCI component may allow a remote attacker to compromise system integrity and availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
MISC: http://www.red-database-security.com/exploits/oracle-sql-injection-oracle-dbms_export_extension.html
CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
MISC: http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
CERT-VN:VU#932124
URL:http://www.kb.cert.org/vuls/id/932124
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

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

CVE Reference: CVE-2006-3702

New Vulnerabilities found this Week

Sun Solaris Kernel Debugger Local Denial of Service
"Denial of Service"

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

The vulnerability is caused due to an unspecified error when the kernel debugger (kmdb) is loaded.

Successful exploitation causes the system to hang.

The vulnerability has been reported in Solaris 10 systems on the x86 platform.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102512-1

Sun Solaris "/net" Mount Point Local Denial of Service
"Denial of Service"

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

The vulnerability is caused due to an unspecified error within the handling of the "/net" mount point (or similarly configured mount points using the "-hosts" special map) and can be exploited to crash the system.

Successful exploitation requires that the system has the autofs service enabled and a "-hosts" entry in the "/etc/auto_master" file.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102286-1

Oracle Products Multiple Vulnerabilities
"SQL injection"

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/critical-patch-updates/cpujul2006.html

http://descriptions.securescout.com/tc/13370
http://descriptions.securescout.com/tc/13371
http://descriptions.securescout.com/tc/13372
http://descriptions.securescout.com/tc/13373
http://descriptions.securescout.com/tc/13374
http://descriptions.securescout.com/tc/13375
http://descriptions.securescout.com/tc/13376
http://descriptions.securescout.com/tc/13377

D-Link Routers UPnP M-SEARCH Request Buffer Overflow
"Buffer overflow"

eEye Digital Security has reported a vulnerability in various D-Link routers, which can be exploited by malicious people to compromise a vulnerable network device.

The vulnerability is caused due to a boundary error in the UPnP service when processing "M-SEARCH" requests. This can be exploited to cause a stack-based buffer overflow by sending an "M-SEARCH" request with an overly long string (about 800 bytes) to port 1900/UDP.

Successful exploitation allows execution of arbitrary code.

References:
http://www.eeye.com/html/research/advisories/AD20060714.html

Linux Kernel "/proc" Race Condition Privilege Escalation
"Gain escalated privileges"

A vulnerability has been reported in the Linux kernel, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to a race condition in "/proc" when changing file status.

Successful exploitation allows execution of arbitrary code with root privileges.

The vulnerability has been reported in versions prior to 2.6.17.5.

References:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.17.5

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