

Table of Contents

[Product Focus](#)

[This Week in Review](#)

[Top Security News Stories this Week](#)

[New Vulnerabilities Tested in SecureScout](#)

[New Vulnerabilities found this Week](#)

Product Focus

[RPC DCOM Vulnerabilities Scanner](#) - The S4 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).

Download Here:

<http://www.netvigilance.com/productdownloads?productname=rpcdcomvulnerabilitiesscanner>

This Week in Review

An example from real life. New security products for the Cloud on the way. They are in great need. DoS attacks - how they do it.

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

• Cyber attackers empty business accounts in minutes

IDG News Service - The criminals knew what they were doing when they hit the Western Beaver County School District.

They waited until school administrators were away on holiday, and then during a four-day period between Dec. 29 and Jan. 2, siphoned US\$704,610.35 out of two of the school district's bank accounts. Western Beaver's financial institution, ESB Bank, managed to reverse some of the transfers, but the Pennsylvania school district was out more than \$441,000.

On July 9, Western Beaver sued ESB to try and recover the money, but security experts say that it's just one of many organizations that have been hit in recent months by a disturbing new type of financial fraud that can often leave the victim holding the bag. Computerworld

Full Story :

http://www.computerworld.com/s/article/9136334/Cyber_attackers_empty_business_accounts_in_minutes?source=r

• Novell, CA Push to Secure Identity, Security in Cloud

CIO - Two major identity management companies are forging ahead with products designed to satisfy what a cloud-computing consortium calls one of the trickiest problems preventing secure and automated connections between internal IT infrastructures and external service providers: identity and authentication.

Last week at The Burton Group's Catalyst Conference, Novell demonstrated a pre-release version of its Cloud Security Service, designed to synchronize login and authentication data between external clouds and internal systems without exposing internal security data.

At the same conference, CA demonstrated a product called Federation Manager, designed to provide single sign-on across several internal and external cloud or SaaS applications. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9136336/Novell CA Push to Secure Identity Security in Cloud?source=rss](http://www.computerworld.com/s/article/9136336/Novell_CA_Push_to_Secure_Identity_Security_in_Cloud?source=rss)

• 5 Lessons from Dark Side of Cloud Computing

CIO - While many companies are considering moving applications to the cloud, the security of the third-party services still leaves much to be desired, security experts warned attendees at last week's Black Hat Security Conference.

The current economic downturn has made cloud computing a hot issue, with startups and smaller firms rushing to save money using virtual machines on the Internet and larger firms pushing applications such as customer relationship management to the likes of Salesforce.com. Yet, companies need to be more wary of the security pitfalls in moving their infrastructure to the cloud, experts say.

"Guys at the low end are using (cloud infrastructure) to save money, but the danger is that the guys at the top end start to use it without any auditing," says Haroon Meer, technical director at security firm SensePost, who discussed his team's research into some aspects of Amazon's Elastic Compute Cloud (EC2) at the Black Hat security conference. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9136337/5 Lessons from Dark Side of Cloud Computing?source=rss](http://www.computerworld.com/s/article/9136337/5_Lessons_from_Dark_Side_of_Cloud_Computing?source=rss)

• FAQ: The ins and outs of DoS attacks

Thursday's denial-of-service attack that knocked Twitter offline for a few hours and affected Facebook, LiveJournal, and Google Sites and Blogger wasn't your average attack.

Typically, someone who has a bone to pick with a specific Web site will round up some hijacked PCs and use them to try to shut the site down. In this case, whoever was responsible was trying to block access to a specific user's accounts and not the sites themselves.

Denial-of-service attacks aren't always straight forward and this one has its own unique twist. Let's take a look at what happened and why. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-10305298-245.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• 13710 Oracle Database Server - Network Foundation component unspecified Vulnerability (jul-2009/CVE-2009-1020)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Network Foundation" component.

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2009.html>

* BID: 35684

<http://www.securityfocus.com/bid/35684>

* OSVDB: 55897

<http://osvdb.org/55897>

* SECTRACK: 1022560

<http://www.securitytracker.com/id?1022560>

* SECUNIA: 35776

<http://secunia.com/advisories/35776>

* VUPEN: ADV-2009-1900
<http://www.vupen.com/english/advisories/2009/1900>

CVE Reference:

CVE-2009-1020 (cve.mitre.org, nvd.nist.gov)

• **13711 Oracle Database Server - Network Authentication component unspecified Vulnerability (jul-2009/CVE-2009-1019)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Network Authentication" component.

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

References:

* CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuijul2009.html>
* BID: 35680
<http://www.securityfocus.com/bid/35680>
* OSVDB: 55884
<http://osvdb.org/55884>
* SECTRAK: 1022560
<http://www.securitytracker.com/id?1022560>
* SECUNIA: 35776
<http://secunia.com/advisories/35776>
* VUPEN: ADV-2009-1900
<http://www.vupen.com/english/advisories/2009/1900>

CVE Reference:

CVE-2009-1019 (cve.mitre.org, nvd.nist.gov)

• **13712 Oracle Database Server - Network Foundation component unspecified Vulnerability (jul-2009/CVE-2009-1963)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Network Foundation" component.

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

References:

* CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuijul2009.html>
* BID: 35677
<http://www.securityfocus.com/bid/35677>
* OSVDB: 55885
<http://osvdb.org/55885>
* SECTRAK: 1022560
<http://www.securitytracker.com/id?1022560>
* SECUNIA: 35776
<http://secunia.com/advisories/35776>
* VUPEN: ADV-2009-1900
<http://www.vupen.com/english/advisories/2009/1900>

CVE Reference:

CVE-2009-1963 (cve.mitre.org, nvd.nist.gov)

• **13713 Oracle Database Server - Advanced Replication component unspecified Vulnerability (jul-2009/CVE-2009-1021)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Advanced Replication" component.

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

References:

* CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuijul2009.html>
* BID: 35685
<http://www.securityfocus.com/bid/35685>
* OSVDB: 55886

<http://osvdb.org/55886>

* SECTrack: 1022560

<http://www.securitytracker.com/id?1022560>

* SECUNIA: 35776

<http://secunia.com/advisories/35776>

* VUPEN: ADV-2009-1900

<http://www.vupen.com/english/advisories/2009/1900>

CVE Reference:

CVE-2009-1021 (cve.mitre.org, nvd.nist.gov)

• **13714 Oracle Database Server - Config Management component unspecified Vulnerability (jul-2009/CVE-2009-1966)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Config Management" component.

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2009.html>

* BID: 35676

<http://www.securityfocus.com/bid/35676>

* OSVDB: 55887

<http://osvdb.org/55887>

* SECTrack: 1022560

<http://www.securitytracker.com/id?1022560>

* SECUNIA: 35776

<http://secunia.com/advisories/35776>

* VUPEN: ADV-2009-1900

<http://www.vupen.com/english/advisories/2009/1900>

CVE Reference:

CVE-2009-1966 (cve.mitre.org, nvd.nist.gov)

• **13715 Oracle Database Server - Config Management component unspecified Vulnerability (jul-2009/CVE-2009-1967)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Config Management" component.

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2009.html>

* BID: 35692

<http://www.securityfocus.com/bid/35692>

* OSVDB: 55888

<http://osvdb.org/55888>

* SECTrack: 1022560

<http://www.securitytracker.com/id?1022560>

* SECUNIA: 35776

<http://secunia.com/advisories/35776>

* VUPEN: ADV-2009-1900

<http://www.vupen.com/english/advisories/2009/1900>

CVE Reference:

CVE-2009-1967 (cve.mitre.org, nvd.nist.gov)

• **13716 Oracle Database Server - Upgrade component unspecified Vulnerability (jul-2009/CVE-2009-0987)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Upgrade" component.

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2009.html>

* BID: 35679
<http://www.securityfocus.com/bid/35679>
* OSVDB: 55889
<http://osvdb.org/55889>
* SECTRACK: 1022560
<http://www.securitytracker.com/id?1022560>
* SECUNIA: 35776
<http://secunia.com/advisories/35776>
* VUPEN: ADV-2009-1900
<http://www.vupen.com/english/advisories/2009/1900>

CVE Reference:

CVE-2009-0987 (cve.mitre.org, nvd.nist.gov)

● **13717 Oracle Database Server - Virtual Private Database component unspecified Vulnerability (jul-2009/CVE-2009-1973)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Virtual Private Database" component.

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

References:

* CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2009.html>
* BID: 35687
<http://www.securityfocus.com/bid/35687>
* OSVDB: 55890
<http://osvdb.org/55890>
* SECTRACK: 1022560
<http://www.securitytracker.com/id?1022560>
* SECUNIA: 35776
<http://secunia.com/advisories/35776>
* VUPEN: ADV-2009-1900
<http://www.vupen.com/english/advisories/2009/1900>

CVE Reference:

CVE-2009-1973 (cve.mitre.org, nvd.nist.gov)

● **13718 Oracle Database Server - Listener component unspecified Vulnerability (jul-2009/CVE-2009-1970)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Listener" component.

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

References:

* CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2009.html>
* BID: 35683
<http://www.securityfocus.com/bid/35683>
* OSVDB: 55891
<http://osvdb.org/55891>
* SECTRACK: 1022560
<http://www.securitytracker.com/id?1022560>
* SECUNIA: 35776
<http://secunia.com/advisories/35776>
* VUPEN: ADV-2009-1900
<http://www.vupen.com/english/advisories/2009/1900>

CVE Reference:

CVE-2009-1970 (cve.mitre.org, nvd.nist.gov)

● **18463 BIND Dynamic Update Denial of Service Vulnerability**

The `dns_db_finddataset` function in `db.c` in `named` in ISC BIND 9.4 before 9.4.3-P3, 9.5 before 9.5.1-P3, and 9.6 before 9.6.1-P1, when configured as a master server, allows remote attackers to cause a denial of service (assertion failure and daemon exit) via an ANY record in the prerequisite section of a crafted dynamic update message, as exploited in the wild in July 2009.

The vulnerability has been fixed in versions 9.4.3-P3, 9.5.1-P3 or 9.6.1-P1.

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

References:

- * CONFIRM: BIND Dynamic Update DoS
<https://www.isc.org/node/474>
- * CERT-VN: VU#725188
<http://www.kb.cert.org/vuls/id/725188>
- * OPENBSD: [4.4] 014: RELIABILITY FIX: July 29, 2009
http://www.openbsd.org/errata44.html#014_bind
- * SUNALERT: 264828
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-264828-1>
- * UBUNTU: USN-808-1
<http://www.ubuntu.com/usn/usn-808-1>
- * SECUNIA: 36053
<http://secunia.com/advisories/36053>

CVE Reference:

CVE-2009-0696 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-2668 Microsoft CVSS 2.0 Score = 7.8

Microsoft Internet Explorer 6 through 6.0.2900.2180 and 7 through 7.0.6000.16473 allows remote attackers to cause a denial of service (CPU consumption) via an XML document composed of a long series of start-tags with no corresponding end-tags, a related issue to CVE-2009-1232.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

- MISC: <http://websecurity.com.ua/3216/>
- BUGTRAQ: <http://archives.neohapsis.com/archives/bugtraq/2009-07/0193.html>

CVE Reference: [CVE-2009-2668](http://cve.mitre.org/cve/2009/2668)

• CVE-2009-2655 Microsoft CVSS 2.0 Score = 5.0

mshtml.dll in Microsoft Internet Explorer 7 and 8 on Windows XP SP3 allows remote attackers to cause a denial of service (application crash) by calling the JavaScript findText method with a crafted Unicode string in the first argument, and only one additional argument, as demonstrated by a second argument of -1.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

- MILWORM: <http://www.milw0rm.com/exploits/9253>

CVE Reference: [CVE-2009-2655](http://cve.mitre.org/cve/2009/2655)

• CVE-2009-2653 Microsoft CVSS 2.0 Score = 4.6

** DISPUTED ** The NtUserConsoleControl function in win32k.sys in Microsoft Windows XP SP2 and SP3, and Server 2003 before SP1, allows local administrators to bypass unspecified "security software" and gain privileges via a crafted call that triggers an overwrite of an arbitrary memory location. NOTE: the vendor disputes the significance of this report, stating that 'the Administrator to SYSTEM "escalation" is not a security boundary we defend.'

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

- MISC: http://www.ntinternals.org/index.html#09_07_30
- MILWORM: <http://www.milw0rm.com/exploits/9301>
- SECTRAK: <http://securitytracker.com/id?1022630>
- MISC: <http://hi.baidu.com/azy0922/blog/item/f950cbc2890729130ef47783.html>

MISC:

<http://blogs.technet.com/srd/archive/2009/06/11/latest-baidu-public-posting-requires-administrator-to-elevate.aspx>

CVE Reference: [CVE-2009-2653](#)

• **CVE-2009-2412 Apache CVSS 2.0 Score = 10.0**

Multiple integer overflows in the Apache Portable Runtime (APR) library and the Apache Portable Utility library (aka APR-util) 0.9.x and 1.3.x allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors that trigger crafted calls to the (1) `allocator_alloc` or (2) `apr_palloc` function in `memory/unix/apr_pools.c` in APR; or crafted calls to the (3) `apr_rmm_malloc`, (4) `apr_rmm_calloc`, or (5) `apr_rmm_realloc` function in `misc/apr_rmm.c` in APR-util; leading to buffer overflows. NOTE: some of these details are obtained from third party information.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

BID: <http://www.securityfocus.com/bid/35949>

CONFIRM: http://svn.apache.org/viewvc/apr/apr/branches/1.3.x/memory/unix/apr_pools.c?r1=678140&r2=800732

CONFIRM: <http://svn.apache.org/viewvc/apr/apr/branches/1.3.x/CHANGES?revision=800732&view=markup>

CONFIRM: http://svn.apache.org/viewvc/apr/apr/branches/0.9.x/memory/unix/apr_pools.c?r1=585356&r2=800733

CONFIRM: <http://svn.apache.org/viewvc/apr/apr/branches/0.9.x/CHANGES?revision=800733&view=markup>

CONFIRM: http://svn.apache.org/viewvc/apr/apr-util/branches/1.3.x/misc/apr_rmm.c?r1=647687&r2=800735

CONFIRM: <http://svn.apache.org/viewvc/apr/apr-util/branches/1.3.x/CHANGES?revision=800735&view=markup>

CONFIRM: http://svn.apache.org/viewvc/apr/apr-util/branches/0.9.x/misc/apr_rmm.c?r1=230441&r2=800736

CONFIRM: <http://svn.apache.org/viewvc/apr/apr-util/branches/0.9.x/CHANGES?revision=800736&view=markup>

SECUNIA: <http://secunia.com/advisories/36140>

SECUNIA: <http://secunia.com/advisories/36138>

CVE Reference: [CVE-2009-2412](#)

• **CVE-2009-2667 IBM CVSS 2.0 Score = 10.0**

Unspecified vulnerability in IBM Tivoli Key Lifecycle Manager (TKLM) 1.0 has unknown impact and attack vectors, related to a "password security vulnerability."

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

VUPEN: <http://www.vupen.com/english/advisories/2009/2144>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21395577>

CVE Reference: [CVE-2009-2667](#)

• **CVE-2009-2669 IBM CVSS 2.0 Score = 7.2**

A certain debugging component in IBM AIX 5.3 and 6.1 does not properly handle the (1) `_LIB_INIT_DBG` and (2) `_LIB_INIT_DBG_FILE` environment variables, which allows local users to gain privileges by leveraging a `setuid-root` program to create an arbitrary root-owned file with world-writable permissions, related to `libC.a` (aka the XL C++ runtime library) in AIX 5.3 and `libc.a` in AIX 6.1.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

BID: <http://www.securityfocus.com/bid/35934>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ56206>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ56205>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ56204>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ56203>

CONFIRM: http://aix.software.ibm.com/aix/efixes/security/libC_advisory.asc

CVE Reference: [CVE-2009-2669](#)

• **CVE-2009-2204 Apple CVSS 2.0 Score = 10.0**

Unspecified vulnerability in the CoreTelephony component in Apple iPhone OS before 3.0.1 allows remote attackers to execute arbitrary code, obtain GPS coordinates, or enable the microphone via an SMS message that triggers memory corruption, as demonstrated by Charlie Miller at SyScan '09 Singapore.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

VUPEN: <http://www.vupen.com/english/advisories/2009/2105>

SECTRAK: <http://securitytracker.com/id?1022626>

MISC: <http://www.syscan.org/Sg/program.html>

BID: <http://www.securityfocus.com/bid/35569>

OSVDB: <http://www.osvdb.org/55687>

MISC: <http://www.blackhat.com/presentations/bh-usa-09/MILLER/BHUSA09-Miller-FuzzingPhone-PAPER.pdf>

CONFIRM: <http://support.apple.com/kb/HT3754>

SECUNIA: <http://secunia.com/advisories/36070>

MISC: http://news.cnet.com/8301-1009_3-10278472-83.html

APPLE: <http://lists.apple.com/archives/security-announce/2009/Jul/msg00001.html>

CVE Reference: [CVE-2009-2204](#)

• **CVE-2009-2193 Apple CVSS 2.0 Score = 10.0**

Buffer overflow in the kernel in Apple Mac OS X 10.5 before 10.5.8 allows remote attackers to execute arbitrary code or cause a denial of service (system crash) via a crafted AppleTalk response packet.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

BID: <http://www.securityfocus.com/bid/35954>

CONFIRM: <http://support.apple.com/kb/HT3757>

APPLE: <http://lists.apple.com/archives/security-announce/2009/Aug/msg00001.html>

CVE Reference: [CVE-2009-2193](#)

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