netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 29

July 27, 2007

Table of Contents

Product Focus

ASN.1 Vulnerability Scanner – The ASN.1 Vulnerability 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 MS04-007 that could allow remote code execution.

This Week in Review

New member in PCI Security Standards Council. New white paper on DNS management. IM becoming the de facto electronic business communication tool. Storm worm active again.

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

- **Motorola joins PCI Security Standards Council**

Motorola's enterprise mobility business is now a member of the Payment Card Industry (PCI) Security Standards Council, which was established in 2004 to help prevent theft of consumers' financial account data in retail environments such as home repair, department and grocery stores.
"Motorola created the first commercial wireless LAN (WLAN) to mobilise retailers' applications for capturing and moving information in real-time. With nearly 20 years of experience, we have extensive expertise building wireless networks for the retail industry," says Sujai Hajela, vice president and general manager, enterprise WLAN division for Motorola's Enterprise Mobility Solutions. "Our involvement and contributions to the PCI Security Standards Council reflects our continued commitment to bringing the best security practices to the market for helping protect consumer account data."

Retail Systems

Full Story :
http://www.retail-systems.com/pages/news_latest/news-latest4.htm#Motorola

- **Analyst Firm Publishes New White Paper Detailing Top DNS Vulnerabilities and How Genuinely Secure DNS Software Can Overcome Them**

A new white paper issued by Hurwitz & Associates entitled, "The 5 Reasons To Worry About Your DNS – Why DNS Technology is Vulnerable and How Genuinely Secure DNS Software Fixes The Problem" is now available.
Researched and authored by two partners at analyst firm Hurwitz & Associates, the in-depth paper identifies and explains five key vulnerabilities that threaten the integrity of today's Domain Name System (DNS) – the backbone of the Internet. It then offers a practical, proactive approach that businesses and organizations can use to protect themselves from these dangerous threats.
Press Releases

Full Story :
http://press-releases.techwhack.com/11412/secure-dns-software/

- **Security focus needed for IM revolution**

With instant messaging (IM) poised to become the de facto electronic business communication tool, small and medium-sized businesses (SMBs) need to get a grip on its security risks.
Gartner predicts that by 2011 instant messaging will be the main conduit through which people will communicate, using video, voice as well as text. It will be so entrenched that by 2013, 95% of workers in leading global companies will use it as their primary way of communicating.
And if SMBs want to do business with those global organisations, they'll have to step up to the plate and adopt technologies to secure and manage IM use.

computerweekly

Full Story :
http://www.computerweekly.com/Articles/2007/07/26/225798/security-focus-needed-for-im-revolution.htm

- **New storm worm run called largest virus attack in two years**

The infamous 'storm worm' virus attack began another run last week, this one called the largest in two years by messaging security vendor Postini.
The San Carlos, Calif.-based company, which Google announced intentions to acquire earlier this month, said this week that the storm worm attack that began July 16 generated 120 million messages by Friday.

Postini said that the attack is spreading through blended methods, using emails that contain links to malicious websites that exploit vulnerabilities.

The attack was named for the deadly European wind storms that occurred simultaneously with the first attacks this past January. Early attacks arrived with video EXE files with storm-related headings, such as "230 dead as storm batters Europe."

SC Magazine

Full Story :
http://www.scmagazine.com/us/news/article/673334/new-storm-worm-run-called-largest-virus-attack-two-years/

New Vulnerabilities Tested in SecureScout

- **16459 Mozilla Firefox - remote code execution by launching Firefox from Internet Explorer (Remote File Checking)**

Internet Explorer calls registered URL protocols without escaping quotes and may be used to pass unexpected and potentially dangerous data to the application that registers that URL Protocol.

The vulnerability is exposed when a user browses to a malicious web page in Internet Explorer and clicks on a specially crafted link. That link causes Internet Explorer to invoke another Windows program via the command line and then pass that program the URL from the malicious webpage without escaping the quotes. Firefox and Thunderbird are among those which can be launched, and both support a "-chrome" option that could be used to run malware.

The issue has been fixed in Firefox 2.0.0.5.

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

References:

References:

* IDEFENSE: 20070719 Multiple Vendor Multiple Product URI Handler Input Validation Vulnerability
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=565
* BUGTRAQ: 20070710 Internet Explorer 0day exploit
http://www.securityfocus.com/archive/1/archive/1/473276/100/0/threaded
* MISC:
http://larholm.com/2007/07/10/internet-explorer-0day-exploit/
* MISC:
http://www.xs-sniper.com/sniperscope/IE-Pwns-Firefox.html
* MISC:
http://blog.mozilla.com/security/2007/07/10/security-issue-in-url-protocol-handling-on-windows/
* MISC:
http://msinfluentials.com/blogs/jesper/archive/2007/07/10/blocking-the-firefox-gt-ie-0-day.aspx
* MISC:
http://www.theregister.co.uk/2007/07/11/ie_firefox_vuln/
* MISC:
http://www.virusbtn.com/news/virus_news/2007/07_11.xml
* CONFIRM:
http://www.mozilla.org/security/announce/2007/mfsa2007-23.html
* CONFIRM:
ftp://ftp.slackware.com/pub/slackware/slackware-12.0/ChangeLog.txt
* CERT-VN: VU#358017
http://www.kb.cert.org/vuls/id/358017
* BID: 24837
http://www.securityfocus.com/bid/24837
* FRSIRT: ADV-2007-2473
http://www.frsirt.com/english/advisories/2007/2473
* FRSIRT: ADV-2007-2565
http://www.frsirt.com/english/advisories/2007/2565
* SECTRACK: 1018351
http://www.securitytracker.com/id?1018351
* SECTRACK: 1018360
http://www.securitytracker.com/id?1018360
* SECUNIA: 25984
http://secunia.com/advisories/25984
* SECUNIA: 26096
http://secunia.com/advisories/26096
* SECUNIA: 26149
http://secunia.com/advisories/26149
* XF: ie-firefoxurl-command-execution(35346)
http://xforce.iss.net/xforce/xfdb/35346
* SECUNIA: 26201
http://secunia.com/advisories/26201/
* MISC:
http://xs-sniper.com/blog/2007/07/24/remote-command-execution-in-firefox-2005/
* MISC:
http://msinfluentials.com/blogs/jesper/archive/2007/07/20/hey-mozilla-quotes-are-not-legal-in-a-url.aspx

* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=384384

CVE Reference: CVE-2007-3670

❖ 16336 BIND Predictable DNS Query IDs Vulnerability

Amit Klein has reported a vulnerability in BIND, which can be exploited by malicious people to poison the DNS cache.

The DNS query id generation is vulnerable to cryptographic analysis which provides a 1 in 8 chance of guessing the next query id for 50% of the query ids. This can be used to perform cache poisoning by an attacker.

This bug only affects outgoing queries, generated by BIND 9 to answer questions as a resolver, or when it is looking up data for internal uses, such as when sending NOTIFYs to slave name servers.

The vulnerability has been fixed in versions 9.2.8-P1, BIND 9.3.4-P1, BIND 9.4.1-P1.

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

References:

* CONFIRM:
http://www.isc.org/index.pl?/sw/bind/bind-security.php
* REDHAT: RHSA-2007:0740
http://www.redhat.com/support/errata/RHSA-2007-0740.html
* FRSIRT: ADV-2007-2627
http://www.frsirt.com/english/advisories/2007/2627
* SECTRACK: 1018442
http://www.securitytracker.com/id?1018442
* SECUNIA: 26152
http://secunia.com/advisories/26152
* MISC:
http://www.trusteer.com/docs/bind9dns_s.html

CVE Reference: CVE-2007-2926

❖ 13559 Oracle Database Server - SQL Compiler component buffer overflow Vulnerability (jul-2007/DB17)

A buffer overflow vulnerability exists in Oracle Database Server SQL Compiler component.

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

References:

* BUGTRAQ: 20070718 BUGTRAQ:20070718 Oracle Security: Insert / Update / Delete Data via Views
http://www.securityfocus.com/archive/1/archive/1/473997/100/0/threaded
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_jul_2007.html
* MISC:
http://www.red-database-security.com/advisory/oracle_view_vulnerability.html
* FRSIRT: ADV-2007-2562
http://www.frsirt.com/english/advisories/2007/2562
* SECUNIA: 26114
http://secunia.com/advisories/26114

CVE Reference: CVE-2007-3855

❖ 13558 Oracle Database Server - Spatial component buffer overflow Vulnerability (jul-2007/DB16)

A buffer overflow vulnerability exists in Oracle Database Server Spatial component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_jul_2007.html
* FRSIRT: ADV-2007-2562
http://www.frsirt.com/english/advisories/2007/2562
* SECUNIA: 26114
http://secunia.com/advisories/26114

CVE Reference: CVE-2007-3855

❖ 13557 Oracle Database Server - Spatial component buffer overflow Vulnerability (jul-2007/DB15)

A buffer overflow vulnerability exists in Oracle Database Server Spatial component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_jul_2007.html
* FRSIRT: ADV-2007-2562
http://www.frsirt.com/english/advisories/2007/2562
* SECUNIA: 26114
http://secunia.com/advisories/26114

CVE Reference: CVE-2007-3853

❖ 13556 Oracle Database Server - JavaVM component buffer overflow Vulnerability (jul-2007/DB14)

A buffer overflow vulnerability exists in Oracle Database Server JavaVM component.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Gather Info** Risk: **Low**

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_jul_2007.html
* FRSIRT: ADV-2007-2562
http://www.frsirt.com/english/advisories/2007/2562
* SECUNIA: 26114
http://secunia.com/advisories/26114

CVE Reference: CVE-2007-3857

❖ 13555 Oracle Database Server - Progam Interface component buffer overflow Vulnerability (jul-2007/DB13)

A buffer overflow vulnerability exists in Oracle Database Server Progam Interface component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html

* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_jul_2007.html
* FRSIRT: ADV-2007-2562
http://www.frsirt.com/english/advisories/2007/2562
* SECUNIA: 26114
http://secunia.com/advisories/26114

CVE Reference: CVE-2007-3858

❖ 13554 Oracle Database Server - Spatial component buffer overflow Vulnerability (jul-2007/DB12)

A buffer overflow vulnerability exists in Oracle Database Server Spatial component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_jul_2007.html
* FRSIRT: ADV-2007-2562
http://www.frsirt.com/english/advisories/2007/2562
* SECUNIA: 26114
http://secunia.com/advisories/26114
* MISC:
http://www.appsecinc.com/resources/alerts/oracle/2007-05.shtml

CVE Reference: CVE-2007-3854

❖ 13553 Oracle Database Server - Rules Manager component buffer overflow Vulnerability (jul-2007/DB11)

Oracle Database Server - Rules Manager component buffer overflow Vulnerability (jul-2007/DB11)

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_jul_2007.html
* FRSIRT: ADV-2007-2562
http://www.frsirt.com/english/advisories/2007/2562

* SECUNIA: 26114
http://secunia.com/advisories/26114

CVE Reference: CVE-2007-3858

❖ **13552 Oracle Database Server - PL/SQL component buffer overflow Vulnerability (jul-2007/DB10)**

A buffer overflow vulnerability exists in Oracle Database Server PL/SQL component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_jul_2007.html
* FRSIRT: ADV-2007-2562
http://www.frsirt.com/english/advisories/2007/2562
* SECUNIA: 26114
http://secunia.com/advisories/26114

CVE Reference: CVE-2007-3855

New Vulnerabilities found this Week

LinkedIn Internet Explorer Toolbar IEContextMenu ActiveX Control Code Execution

"Execute arbitrary code"

Jared DeMott and Justin Seitz have discovered a vulnerability in LinkedIn Internet Explorer Toolbar, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an error within the IEToolbar.IEContextMenu.1 (LinkedInIEToolbar.dll) when handling the "Search()" method, which takes in a VARIANT as the "varBrowser" argument. This can be exploited to execute arbitrary code when a user e.g. visits a malicious website.

The vulnerability is confirmed in version 3.0.2.1098. Other versions may also be affected.

References:
http://www.vdalabs.com/tools/linkedin.html

CA eTrust Intrusion Detection CallCode ActiveX Control Insecure Methods

“Execute arbitrary code”

Some vulnerabilities have been reported in CA eTrust Intrusion Detection, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerabilities are caused due to the CallCode (caller.dll) ActiveX control including certain insecure methods, which allow loading of arbitrary DLL files and calling the exported functions with controlled parameters. This can be exploited to e.g. execute arbitrary code when a user visits a malicious website.

The vulnerabilities affect the following products:
* eTrust Intrusion Detection 3.0
* eTrust Intrusion Detection 3.0 SP1

References:
http://supportconnectw.ca.com/public/etrust/etrust_intrusion/infodocs/eid-callervilnsecnot.asp
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=568

Mozilla Firefox - remote code execution by launching Firefox from Internet Explorer

“Remote code execution”

Internet Explorer calls registered URL protocols without escaping quotes and may be used to pass unexpected and potentially dangerous data to the application that registers that URL Protocol.

The vulnerability is exposed when a user browses to a malicious web page in Internet Explorer and clicks on a specially crafted link. That link causes Internet Explorer to invoke another Windows program via the command line and then pass that program the URL from the malicious webpage without escaping the quotes. Firefox and Thunderbird are among those which can be launched, and both support a "-chrome" option that could be used to run malware.

The issue has been fixed in Firefox 2.0.0.5.

References:
http://larholm.com/2007/07/10/internet-explorer-0day-exploit/
http://www.xs-sniper.com/sniperscope/IE-Pwns-Firefox.html
http://blog.mozilla.com/security/2007/07/10/security-issue-in-url-protocol-handling-on-windows/
http://msinfluentials.com/blogs/jesper/archive/2007/07/10/blocking-the-firefox-gt-ie-0-day.aspx
http://www.mozilla.org/security/announce/2007/mfsa2007-23.html
http://www.kb.cert.org/vuls/id/358017
https://bugzilla.mozilla.org/show_bug.cgi?id=384384
http://descriptions.securescout.com/tc/16459

McAfee VirusScan ZIP Decompression Vulnerability

“Execute arbitrary code”

Tavis Ormandy has discovered a vulnerability in McAfee VirusScan, which potentially can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to the improper handling of dynamic Huffman coding within the ZIP decompression mechanism. This can potentially be exploited to execute arbitrary code with the permissions of a user scanning a specially crafted ZIP file.

The vulnerability is confirmed in McAfee VirusScan Command Line Scanner for Linux evaluation version 5.10 and is also reported in McAfee VirusScan for Windows. Other versions may also be affected.

References
http://secunia.com/advisories/26137/

BIND Predictable DNS Query IDs Vulnerability
"Cache poisoning"

Amit Klein has reported a vulnerability in BIND, which can be exploited by malicious people to poison the DNS cache.

The DNS query id generation is vulnerable to cryptographic analysis which provides a 1 in 8 chance of guessing the next query id for 50% of the query ids. This can be used to perform cache poisoning by an attacker.

This bug only affects outgoing queries, generated by BIND 9 to answer questions as a resolver, or when it is looking up data for internal uses, such as when sending NOTIFYs to slave name servers.

The vulnerability has been fixed in versions 9.2.8-P1, BIND 9.3.4-P1, BIND 9.4.1-P1.

References:
http://www.isc.org/index.pl?/sw/bind/bind-security.php
http://descriptions.securescout.com/tc/16336

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