netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 21

June 1, 2007

Table of Contents

Product Focus

Mydoom Worm Scanner – The S4 MyDoom Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any have been infected by the MyDoom email virus or its variants.

This Week in Review

This week netVigilance Security Research has found 3 vulnerabilities in open source software Jetbox Contents Management System:

1 high risk, 1 medium risk and 1 low risk. The vulnerabilities include SQL Injection, XSS (Cross site Scripting) and Path Disclosure Vulnerabilities.

To see details and further information please see:
http://www.netvigilance.com/advisories

netvigilance releases WinHoneyd 1.5 with all the features of Honeyd. We also offer a commercial GUI for those not interested in dealing with complex configurations.
This is how infoworld reacts:

Honeyd Fixed and Ported to Windows

I could not be more excited. Years ago, Michael Davis ported an early version of Honeyd (www.honeyd.org) to Windows as part of a Honeyd contest. It was an admirable attempt, but contained so many bugs that it really couldn't be used as a proper honeypot. As Windows changed versions, the older, ported, version of Honeyd remained the same, with bugs and less features than it's Linux/Unix/BSD counterpart. Every since my book, Honeypots for Windows, was published, I've been recommending Honeyd on Linux or OpenBSD for users who want to use Honeyd. Since most Windows users don't have nix

skills, it was a lot to ask.
It was announced today that Jesper Jurcenoks with netVigilance has ported the latest, and feature rich version of Honeyd, and it is available for free download (registration is required).
They have also created an optional $99 GUI configurator. If you're new to Honeyd and want to have less problems, buy the gui and support the vendor.

infoworld

http://weblog.infoworld.com/securityadviser/archives/2007/05/honeyd_fixed_an.html

Malware attacks 9,500 web pages every day. Spammers constantly take new routes. Microsoft and security. What is 'Responsible Disclosure'?

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

- **Hack Attack: 9,500 new infected web pages every day, reports Sophos**

  Sophos, a world leader in IT security and control, has revealed the most prevalent malware threats causing problems for computer users around the world during May 2007.

  The figures compiled by Sophos's global network of monitoring stations show that infected web pages continue to pose a threat, affecting official government websites as well as other legitimate pages. On average this month, Sophos uncovered 9,500 new infected web pages daily - an increase of more than 1000 every day when compared to April. In total, 304,000 web pages hosting malicious code were identified in May.

  The top ten list of web-based malware threats in May 2007 reads as follows:

sophos

Full Story :
http://www.sophos.com/pressoffice/news/articles/2007/06/toptenmay07.html?_log_from=rss

- **Spammers establishing use of artificial intelligence**

Though security industry experts were freely predicting the death of spam several years ago, the arrival of image-based attacks has resulted in a stunning renaissance in the volumes of unwanted e-mail reaching end-users' inboxes.

And while filtering technologies have improved significantly and can thwart the ability of most image spam to force its way onto corporate networks today, some experts believe that the fight against the use of such AI (artificial intelligence) tactics on the part of spammers is only just getting underway.

In a report published on May 30, analysts at Cambridge, Mass.-based Forrester Research elaborate on their theory that image spam is merely the tip of the iceberg when it comes to spammers' use of AI.

The only way to prevent a repeat of the image spam surge as new models using AI come to light, Forrester analysts said, will be for technology vendors and enterprise customers to abandon their current approach of trying to filter out every type of campaign that the mass-mailers conceive and instead battle the roots of the problem.

computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9022560&taxonomyId=17&intsrc=kc_top

❖ Microsoft Doesn't Do Security – It Does Culture...

Microsoft doesn't do security, and although the company has publicized Windows Vista as the most secure Windows platform to date, the operating system is in fact the first product of the culture change business over in Redmond. This is the perspective of a 17-year Microsoft veteran. David Ladd, Senior Security Program Manager on the Security Engineering Strategy Team offered a unique perspective over Microsoft's Security Development Lifecycle as a culture change business.

The Security Development Lifecycle is nothing more than a framework of processes and technologies, and in this sense, it is innovative because nobody before Microsoft has managed to focus and centralize security methodologies into a comprehensive architecture.

"Microsoft has two things going for it in this regard; strong executive support and the unfortunate experience gained by living through "tectonic" security events – which have snapped trustworthiness issues into razor-sharp focus and continue to provide motivation by the truckload. This clarity of thought at the executive level has allowed us to create, implement, and refine the SDL – providing resources and support at critical junctures has proven to be absolutely vital in driving culture change at Microsoft," Ladd explained.

softpedia

Full Story :
http://news.softpedia.com/news/Microsoft-Doesn-039-t-Do-Security-It-Does-Culture-56186.shtml

❖ Security flap: 'Responsible disclosure' debate flares anew

When a recent hacking contest won security researcher Dino Dai Zovi a $10,000 award for breaking into a MacBook Pro computer by exploiting a flaw he'd discovered, the contest reignited a long-simmering debate over "responsible disclosure" of vulnerabilities. Research firm Gartner denounced public hacking contests as an inappropriate way to

conduct vulnerability research, noting such contests can run "contrary to responsible-disclosure practices" that give vendors a chance to develop patches or remediation before public announcements. TippingPoint paid the $10,000 award for the conference-run contest and found itself under fire from competitors, including McAfee and Internet Security Systems, both of which oppose paying rewards for vulnerability discoveries.

networkworld

Full Story :
http://www.networkworld.com/news/2007/053107-security-flap.html?fsrc=netflash-rss

New Vulnerabilities Tested in SecureScout

- **13538 Oracle Database Server - Change Data Capture (CDC) component SQL Injection Vulnerability (apr-2007/DB09)**

An SQL injection vulnerability exists in Oracle Database Server Change Data Capture (CDC) component.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html

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

CVE Reference: CVE-2007-2115

- **13537 Oracle Database Server - Change Data Capture (CDC) component Buffer Overflow Vulnerability (apr-2007/DB08)**

A buffer overflow vulnerability exists in Oracle Database Server Change Data Capture (CDC) component.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html

Other references:

http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html

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

CVE Reference:

❖ 13536 Oracle Database Server - Oracle Agent component unknown impact Vulnerability (apr-2007/EM01)

A vulnerability exists in Oracle Database Server Oracle Agent component.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.htm

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html

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

CVE Reference: CVE-2007-2129

❖ 13535 Oracle Database Server - Upgrade/Downgrade component SQL Injection Vulnerability (apr-2007/DB07)

An SQL injection vulnerability exists in Oracle Database Server Upgrade/Downgrade component.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html

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

CVE Reference: CVE-2007-2113

❖ 13534 Oracle Database Server - Oracle Streams component SQL Injection Vulnerability (apr-2007/DB06)

An SQL injection vulnerability exists in Oracle Database Server Oracle Streams component.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html

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

CVE Reference: CVE-2007-2109

❖ 13533 Oracle Database Server - Authentication component security bypass Vulnerability (apr-2007/DB05)

A security bypass vulnerability exists in Oracle Database Server Authentication component.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html

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

CVE Reference: CVE-2007-2112

❖ 13532 Oracle Database Server - Advanced Queuing component SQL Injection Vulnerability (apr-2007/DB04)

An SQL injection vulnerability exists in Oracle Database Server Advanced Queuing component.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html

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

CVE Reference: CVE-2007-2111

❖ 13531 Oracle Database Server - Core RDBMS component code execution Vulnerability (apr-2007/DB03)

A code execution vulnerability exists in Oracle Database Server Core RDBMS component.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html

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

CVE Reference: CVE-2007-2110

❖ 13530 Oracle Database Server - Rules Manager, Expression Filter component Race Condition Vulnerability (apr-2007/DB02)

A race condition vulnerability exists in Oracle Database Server Rules Manager, Expression Filter component.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html

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

CVE Reference: CVE-2007-2109

- **13529 Oracle Database Server - Core RDBMS component Authentication Bypass via Windows Share Vulnerability (apr-2007/DB01)**

A vulnerability exists in Oracle Database Server Core RDBMS component, due to the way that Windows XP with Simple File Sharing enabled logs on users. It is possible for an attacker to gain DBA access to the Oracle server.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html

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

CVE Reference: CVE-2007-2108

New Vulnerabilities found this Week

Apple QuickTime Java Extension Two Vulnerabilities

"Execution of arbitrary code"

Two vulnerabilities have been reported in Apple QuickTime, which can be exploited by malicious people to gain knowledge of potentially sensitive information or compromise a user's system.

1) A design error in the security restrictions on subclasses of QTObject can be exploited by untrusted Java code to allow subclassing of QuickTime objects that call unsafe functions from QTJava.dll resulting in reading and writing of arbitrary memory.

Successful exploitation allows execution of arbitrary code on Windows and OS X systems when a user visits a malicious web site using a Java-enabled browser.

2) A design error within the handling of Java applets can be exploited to read the

browser's memory when a user visits a malicious website containing a malicious Java applet.

References:
http://docs.info.apple.com/article.html?artnum=305531
http://secunia.com/secunia_research/2007-52/
http://www.kb.cert.org/vuls/id/434748
http://www.kb.cert.org/vuls/id/995836

Mozilla Firefox Multiple Vulnerabilities
"Execute arbitrary code; conduct spoofing attacks"

Some vulnerabilities have been reported in Mozilla Firefox, which can be exploited by malicious people to conduct spoofing attacks, bypass certain security restrictions, and potentially compromise a user's system.

1) Errors in the JavaScript engine can be exploited to cause memory corruption and potentially to execute arbitrary code.

2) An error in the "addEventListener" method can be exploited to inject script into another site, circumventing the browser's same-origin policy. This could be used to access or modify sensitive information from the other site.

3) An error in the handling of XUL popups can be exploited to spoof parts of the browser such as the location bar.

References:
http://www.mozilla.org/security/announce/2007/mfsa2007-12.html
http://www.mozilla.org/security/announce/2007/mfsa2007-16.html
http://www.mozilla.org/security/announce/2007/mfsa2007-17.html
http://www.kb.cert.org/vuls/id/751636

F-Secure Products LHA Archive Handling Buffer Overflow
"Execution of arbitrary code"

A vulnerability has been reported in various F-Secure products, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the processing of LHA archives and can be exploited to cause a buffer overflow when decompressing a specially crafted archive.

Successful exploitation may allow execution of arbitrary code.

References:
http://www.f-secure.com/security/fsc-2007-1.shtml

Sun Java System Web Proxy Server SOCKS Module Buffer Overflows
"Execution of arbitrary code"

Two vulnerabilities have been reported in Sun Java System Web Proxy Server, which can

be exploited by malicious people to compromise a vulnerable system.

The vulnerabilities are caused due to boundary errors within the SOCKS module and can be exploited to cause stack-based buffer overflows by sending specially crafted packets to the SOCKS server.

Successful exploitation allows execution of arbitrary code.

The vulnerabilities are reported in versions 4.0.4 and prior.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102927-1
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=536
http://www.kb.cert.org/vuls/id/746889

Apple Mac OS X Security Update for Multiple Vulnerabilities

"Denial of Service; Execute arbitrary code; Disclose information"

Apple has issued a security update for Mac OS X, which fixes multiple vulnerabilities.

1) Alias Manager does not display identically-named files contained in identically-named mounted disk images. This can be exploited by malicious people to execute a malicious application by tricking a user into mounting two identically-named disk images.

2) Some errors in BIND can be exploited by malicious people to cause a DoS (Denial of Service).

3) An integer overflow error in CoreGraphics when processing a PDF file can be exploited by malicious people to execute arbitrary code.

This does not affect systems prior to Mac OS X v10.4.

4) An error in crontabs may cause a DoS when filesystems mounted in /tmp gets deleted when the daily cleanup script is executed.

5) An error within the APOP implementation of fetchmail may be exploited by malicious people to disclose a user's password.

6) An integer underflow error within file's "file_printf" function can be exploited by malicious people to cause a heap-based buffer overflow.

7) An error in iChat's UPnP IGD (Internet Gateway Device Standardized Device Control Protocol) module can be exploited by malicious people to cause a buffer overflow by sending a specially crafted packet to the application.

8) An error in mDNSResponder's UPnP IGD (Internet Gateway Device Standardized Device Control Protocol) module can be exploited by malicious people to cause a buffer overflow by sending a specially crafted packet to the application.

This does not affect systems prior to Mac OS X v10.4.

9) Insufficient access validation in pppd when processing the "plugin" command line option can be exploited by malicious, local users to load arbitrary plugins and gain escalated privileges.

This does not affect systems prior to Mac OS X v10.4.

10) Two vulnerabilities in ruby can be exploited by malicious people to cause a DoS.

11) Errors in screen can be exploited by malicious people to cause a DoS or potentially compromise a vulnerable system.

12) An error in texinfo can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges.

13) A format string error in vpnd can be exploited by malicious, local users to gain escalated privileges by running vpnd with specially crafted arguments.

References:
http://docs.info.apple.com/article.html?artnum=305530
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=537
http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-mac-os-x/

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