netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 25

June 29, 2007

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

Sasser Worm Scanner – The Sasser Worm 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 SSL Vulnerability (MS04-011) that used by the Sasser Worm to infect machines.

This Week in Review

This week netVigilance Security Research has found 3 vulnerabilities in open source software eTicket and Calendarix:

1 high risk, 2 medium risk and 4 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

Discussion on malware on IIS versus Apache. Is there any way to detect virtualization-based rootkits? Wanted: More security between platforms.MS site hacked.

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

❖ IIS vs. Apache: Re-examining the statistics

Can IP addresses ever be used for accurate statistical analysis of malicious Web sites?
As a Microsoft employee, I try to avoid writing on areas that blatantly promote Microsoft. However, I think this question is generic enough to involve Microsoft in the discussion: Can IP addresses ever be used for statistical analysis of malicious Web sites?
I've been a malware fighter for more than 20 years. I consider myself fairly up-to-date on the subject of malicious mobile code, malware, hackers, and exploitation vectors in general.

So it was with surprise then that I read another of Google's recent studies purporting that IIS Web servers were twice as likely to contain malware as Apache Web servers (although Apache and IIS Web servers contained malicious Web sites in equal numbers).

infoworld

Full Story :
http://www.infoworld.com/article/07/06/29/26OPsecadvise_1.html?source=rss&url=http://www.infoworld.com/article/07/06/29/26OPsecadvise_1.html

❖ Get Ready For A Hacker Smackdown

A showdown is brewing between two sets of security researchers over whether virtualization-based rootkits are detectable in a system or not.
A showdown is brewing between two sets of security researchers over whether virtualization-based rootkits are detectable in a system or not.

A trio of researchers has publicly challenged Joanna Rutkowska, who made a name for herself at last year's Black Hat USA conference for cracking the kernel in Microsoft's Windows Vista beta release and since has led groundbreaking research in stealth malware, to let them prove that they can indeed detect her homegrown stealth virtual machine code called Blue Pill. They have offered her two shrink-wrapped laptops of her choice, one of which she would infect with Blue Pill. If they can't find the laptop with the stealth malware, she gets to keep the machines.

But the contest, proposed to take place at Black Hat USA in July, probably won't materialize -- at least in the near-term. It was the brainchild of Thomas Ptacek, co-founder and researcher with Matasano Security; Nate Lawson, researcher at Root Labs; and Peter Ferrie, senior researcher at Symantec, to disprove Rutkowksa's claims that there's no way to detect this type of malware.

informationweek

Full Story :
http://www.informationweek.com/news/showArticle.jhtml;jsessionid=QKSK3Q0CL2B1GQSNDLOSKH0CJUNN2JVN?articleID=200001635&subSection=News

❖ Vendors admit more cooperation needed on security

The security chiefs of several large infrastructure and software vendors said they are doing all they can do to embed security into their products, but they agreed that more work must be done to improve security between their platforms.

Even though vendors have built in security controls to narrow the gap between their products and their partner products, gaps remain. That makes it difficult for IT security professionals to manage multiple platforms and secure transactions between various applications and servers.
In a roundtable discussion with attendees at the Burton Group Catalyst Conference Wednesday, the security chiefs from Oracle, CA., Microsoft, EMC's RSA division and intrusion prevention system vendor Third Brigade said their organisstions are working to be more proactive about security. Still, conference attendees said growing heterogeneous environments and the explosion of Web-based applications has made security difficult to control.

computerweekly

Full Story :
http://www.computerweekly.com/Articles/2007/06/29/225186/vendors-admit-more-cooperation-needed-on-security.htm

❖ Microsoft British site hacked

A hacker has successfully attacked a web page within Microsoft UK domain, resulting in the display of a photograph of a child waving the flag of Saudi Arabia.

It was "unfortunate" that the site was vulnerable, said Roger Halbheer, chief security advisor for Microsoft in Europe, the Middle East and Africa.

The problem has since been fixed. However, the hack highlights how large software companies with technical expertise can still prove vulnerable to hackers.

The hacker, who posted his name as "rEmOtEr," exploited a programming mistake in the site by using a technique known as SQL injection to get unauthorised access to a database, Halbheer said. The site took SQL queries of a particular form, embedded in URLs (uniform resource locators), and passed them to a database. By embedding a query with an unexpected form in the requested URL, the hacker prompted the server to return error messages, Halbheer said.

techworld

Full Story :
http://www.techworld.com/security/news/index.cfm?newsID=9336&pagtype=all

New Vulnerabilities Tested in SecureScout

❖ 16536 Linux Kernel VFAT IOCTLs Denial of Service Vulnerability

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

The security issue is caused due to an error within the handling of certain VFAT IOCTLs on 64bit systems, which can be exploited to crash the kernel by calling certain IOCTLs with malicious parameters.

Successful exploitation requires a 64bit-system and vfat and msdos file systems.

The vulnerability is reported in versions prior to 2.6.21.2.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.21.2

Other references:
BID:24134
URL:http://www.securityfocus.com/bid/24134
FRSIRT:ADV-2007-2023
URL:http://www.frsirt.com/english/advisories/2007/2023
SECUNIA:25505
URL:http://secunia.com/advisories/25505

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2007-2878

❖ 16535 Linux Kernel "compat_sys_mount()" Denial of Service Vulnerability

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

The security issue is caused due to a NULL pointer dereference error in the "compat_sys_mount()" function in fs/compat.c, which can be exploited to crash a vulnerable system by mounting an smbfs file system in compatibility mode.

The vulnerability is reported in versions prior to 2.6.21.1.

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

References:

Original advisory:
http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff_plain;h=822191a2fa1584a29c3224ab328507adcaeac1ab

Other references:
REDHAT:RHSA-2007:0376
URL:https://rhn.redhat.com/errata/RHSA-2007-0376.html
REDHAT:RHSA-2007:0488
URL:http://rhn.redhat.com/errata/RHSA-2007-0488.html
SUSE:SUSE-SA:2007:035
URL:http://www.novell.com/linux/security/advisories/2007_35_kernel.html
FRSIRT:ADV-2007-2209
URL:http://www.frsirt.com/english/advisories/2007/2209
SECUNIA:25682
URL:http://secunia.com/advisories/25682
SECUNIA:25700
URL:http://secunia.com/advisories/25700
SECUNIA:25683
URL:http://secunia.com/advisories/25683

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-7203

❖ 16534 Linux Kernel "sysfs_readdir()" Denial of Service Vulnerability

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

The vulnerability is caused due to a NULL pointer dereference within the function "sysfs_readdir()" when handling pointers to inodes. This can be exploited to crash a vulnerable system.

The vulnerability is reported in versions prior to 2.6.21.5.

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

References:

Original advisory:
* REDHAT:RHSA-2007:0488
http://rhn.redhat.com/errata/RHSA-2007-0488.html

Other references:
* MISC: http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=242558
* SECUNIA:25771
* URL:http://secunia.com/advisories/25771

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2007-3104

❖ 16533 Wireshark Off-by-one error in the DHCP/BOOTP dissector Denial of Service Vulnerability (Remote File Checking)

Description: Off-by-one error in the DHCP/BOOTP dissector in Wireshark before 0.99.6 allows remote attackers to cause a denial of service (crash) via crafted DHCP-over-DOCSIS packets.

The vulnerability has been reported in versions 0.10.1 to 0.99.5.

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

References:

Original Advisory:
http://www.wireshark.org/docs/relnotes/wireshark-0.99.6.html
http://www.wireshark.org/security/wnpa-sec-2007-02.html

Other references:
http://www.securityfocus.com/bid/24662

Product Homepage:
http://www.wireshark.org/

CVE Reference: CVE-2007-3393

❖ 16532 Wireshark malformed SSL or MMS packets Denial of Service Vulnerability (Remote File Checking)

Wireshark before 0.99.6 allows remote attackers to cause a denial of service via malformed (1) SSL or (2) MMS packets that trigger an infinite loop.

The vulnerability has been reported in versions 0.10.1 to 0.99.5.

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

References:

Original Advisory:
http://www.wireshark.org/docs/relnotes/wireshark-0.99.6.html
http://www.wireshark.org/security/wnpa-sec-2007-02.html

Other references:
http://www.securityfocus.com/bid/24662

Product Homepage:
http://www.wireshark.org/

CVE Reference: CVE-2007-3392

❖ 16531 Wireshark malformed DCP ETSI packet Denial of Service Vulnerability (Remote File Checking)

Wireshark 0.99.5 allows remote attackers to cause a denial of service (memory consumption) via a malformed DCP ETSI packet that triggers an infinite loop.

The vulnerability has been reported in version 0.99.5.

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

References:

Original Advisory:
http://www.wireshark.org/docs/relnotes/wireshark-0.99.6.html
http://www.wireshark.org/security/wnpa-sec-2007-02.html

Other references:
http://www.securityfocus.com/bid/24662

Product Homepage:
http://www.wireshark.org/

CVE Reference: CVE-2007-3391

❖ 16530 Wireshark iSeries capture files Denial of Service Vulnerability (Remote File Checking)

Wireshark 0.10.14 to 0.99.5, when running on certain systems, allows remote attackers to cause a denial of service (crash) via crafted iSeries capture files that trigger a SIGTRAP.

The vulnerability has been reported in versions 0.10.14 to 0.99.5.

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

References:

Original Advisory:
http://www.wireshark.org/docs/relnotes/wireshark-0.99.6.html
http://www.wireshark.org/security/wnpa-sec-2007-02.html

Other references:
http://www.securityfocus.com/bid/24662

Product Homepage:
http://www.wireshark.org/

CVE Reference: CVE-2007-3390

❖ 16486 Wireshark HTTP chunked responses Denial of Service Vulnerability (Remote File Checking)

Wireshark before 0.99.5 allows remote attackers to cause a denial of service (crash) via a crafted chunked encoding in an HTTP response, possibly related to a zero-length payload.

The vulnerability has been reported in version 0.99.5.

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

References:

Original Advisory:
http://www.wireshark.org/docs/relnotes/wireshark-0.99.6.html
http://www.wireshark.org/security/wnpa-sec-2007-02.html

Other references:
http://www.securityfocus.com/bid/24662

Product Homepage:
http://www.wireshark.org/

CVE Reference: CVE-2007-3389

❖ 16180 RealPlayer (10.5/10.5 Beta/10/8) SMIL wallclock Buffer Overflow Vulnerability (Remote File Checking)

A vulnerability has been reported in RealPlayer and Helix Player, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the wallclock functionality in "SmilTimeValue::parseWallClockValue()" when handling time formats. This can be exploited to cause a stack-based buffer overflow via an SMIL file with an overly long, specially-crafted time string.

Successful exploitation allows execution of arbitrary code when a user e.g. visits a malicious website.

The vulnerability is reported in RealPlayer 10.5-GOLD. Other versions may also be affected.

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

References:

Original Advisories:
* IDEFENSE:20070626 RealNetworks RealPlayer/HelixPlayer SMIL wallclock Stack Overflow Vulnerability
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=547

Other references:
http://secunia.com/advisories/25819/
http://www.securityfocus.com/bid/24658

Product HomePage:
http://service.real.com/realplayer/security/

CVE Reference: CVE-2007-3410

❖ **14055 Samba smbd multiple heap-based buffer overflows in the NDR parsing**

Multiple heap-based buffer overflows in the NDR parsing in smbd in Samba 3.0.0 through 3.0.25rc3 allow remote attackers to execute arbitrary code via crafted MS-RPC requests involving (1) DFSEnum (netdfs_io_dfs_EnumInfo_d), (2) RFNPCNEX (smb_io_notify_option_type_data), (3) LsarAddPrivilegesToAccount (lsa_io_privilege_set), (4) NetSetFileSecurity (sec_io_acl), or (5) LsarLookupSids/LsarLookupSids2 (lsa_io_trans_names).

The security issue has been fixed in version 3.0.25.

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

References:

Initial advisory:
MISC: http://www.zerodayinitiative.com/advisories/ZDI-07-029.html
MISC: http://www.zerodayinitiative.com/advisories/ZDI-07-030.html
MISC: http://www.zerodayinitiative.com/advisories/ZDI-07-031.html
MISC: http://www.zerodayinitiative.com/advisories/ZDI-07-032.html
MISC: http://www.zerodayinitiative.com/advisories/ZDI-07-033.html

CVE Reference: CVE-2007-2446

New Vulnerabilities found this Week

Apple Mac OS X Security Update for Two Vulnerabilities

"Execute arbitrary code"

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

1) An invalid type conversion when rendering frame sets in WebKit can be exploited to corrupt memory and can be exploited to execute arbitrary code when a user visits a malicious website.

2) An input validation error in the processing of headers passed to the "XMLHttpRequest" object in WebCore can be exploited to inject arbitrary HTTP requests.

References:
http://docs.info.apple.com/article.html?artnum=305759
http://www.westpoint.ltd.uk/advisories/wp-07-0002.txt
http://www.kb.cert.org/vuls/id/845708
http://www.kb.cert.org/vuls/id/389868

Blackberry Multiple Denial of Service Vulnerabilities

"Denial of Service"

Sipera VIPER Lab has reported some vulnerabilities in Blackberry, which can be exploited by malicious people to cause a DoS (Denial of Service).

1) A format string error in the handling of SIP INVITE messages can be exploited to prevent the BlackBerry smartphone from making a call by sending a specially crafted SIP INVITE message containing a URI with a user name but no host name in the Contact header.

2) An error exists in the processing of SIP INVITE messages can be exploited to prevent the BlackBerry smartphone from clearing the INVITE transaction state properly resulting in the phone being blocked for approximately 40 seconds.

3) An error in the handling of SIP INVITE messages can be exploited to prevent the BlackBerry smartphone from making a call by sending a specially crafted SIP INVITE message.

Successful exploitation of these vulnerabilities requires access to a private branch exchange (PBX) from within an enterprise network.

The vulnerabilities are reported in the BlackBerry Device Software 4.0 Service Pack 1 Bundle 83 and earlier on a BlackBerry 7270 smartphone. Reportedly this does not affect any other BlackBerry device.

References:
http://www.sipera.com/index.php?action=resources,threat_advisory&tid=208
http://www.sipera.com/index.php?action=resources,threat_advisory&tid=213
http://www.sipera.com/index.php?action=resources,threat_advisory&tid=211
http://www.blackberry.com/btsc/articles/218/KB12707_f.SAL_Public.html
http://www.blackberry.com/btsc/articles/220/KB12705_f.SAL_Public.html
http://www.blackberry.com/btsc/articles/225/KB12700_f.SAL_Public.html

RealPlayer/Helix Player SMIL wallclock Buffer Overflow Vulnerability

"Execution of arbitrary code"

A vulnerability has been reported in RealPlayer and Helix Player, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the wallclock functionality in "SmilTimeValue::parseWallClockValue()" when handling time formats. This can be exploited to cause a stack-based buffer overflow via an SMIL file with an overly long, specially-crafted time string.

Successful exploitation allows execution of arbitrary code when a user e.g. visits a malicious website.

The vulnerability is reported in RealPlayer 10.5-GOLD. Other versions may also be affected.

References:
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=547

http://www.kb.cert.org/vuls/id/770904

Nessus Unspecified Cross-Site Scripting Vulnerability
"Cross-site scripting attacks"

A vulnerability has been reported in Nessus, which can be exploited by malicious people to conduct cross-site scripting attacks.

Unspecified input within the Windows GUI is not properly sanitized before being returned to a user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

References:
http://www.nessus.org/news/

Nortel PC Client SIP Soft Phone Denial of Service
"Denial of Service"

Sipera VIPER Lab has reported a vulnerability in Nortel PC Client SIP Soft Phone, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the SIP header parsing module and can be exploited to crash the application via a specially crafted SIP message containing a malformed header.

The vulnerability is reported in release 4.1 version 3.5.208[20051015]. Other versions may also be affected.

References:
http://www.sipera.com/index.php?action=resources,threat_advisory&tid=298&

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