netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 25

June 24, 2006

Table of Contents

Product Focus

CodeRed Worm Scanner – The CodeRed 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 CodeRed Worm.

This Week in Review

Wi-fi hacking and abuse, malware attacks web applications, EU into security.

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

- **Man arrested for abusing wireless Internet access**

The law is starting to side with the uninformed more often in the wireless world, as evident by the reactions of people to war driving and getting wireless connections they shouldn't. Most recently, there's a story from my local area about a man who has been arrested for using free Internet access too much. A coffee shop in Vancouver, Washington had a

service that many other companies also offer – free Internet access while you're on the premises. This was intended for customer use only, of course. But like many who operate free access points, they didn't enforce any type of protection on it. As a result, the man began using the service for free, for three months. Despite complaints and warnings, he kept doing it, and is now in jail.

techspot

Full Story :

http://www.techspot.com/news/21986-man-arrested-for-abusing-wireless-internet-access.html

❖ Wi-Fi drivers open laptops to hackers

Hackers can take control of laptops by Wi-Fi, even when the user is not connected to a wireless LAN, according to security researchers.

The hack, which exploits bugs in wireless device drivers, will be demonstrated at the upcoming Black Hat USA 2006 conference during a presentation by David Maynor, a research engineer with Internet Security Systems, and Jon Ellch, a student at the US Naval postgraduate school in Monterey, California.

Device driver hacking is technically challenging, but the field has become more appealing in recent years, thanks in part to new software tools that make it easier for less technically savvy hackers, known as script kiddies, to attack wireless cards, Maynor said in an interview.

IDG News

Full Story :

http://www.techworld.com/mobility/news/index.cfm?newsID=6272&pagtype=all

❖ Malware authors eyeing Web-based applications

Malware attacks against search giants Yahoo and Google this past week show online outlaws are working overtime to exploit any security hole they can find in Web applications. As Web-based services grow increasingly popular, industry experts say users should brace for more of these threats.

Last week, Yahoo Mail was targeted by a JavaScript worm called JS.Yamanner, which spread through Yahoo email contacts when end-users opened emails infected by the malware.

Also in recent days, Google Inc. has tried to fight off malware targeting its Google Page Creator Web site hosting service as well as its Orkut social networking service. The attacks illustrate a growing trend where the digital underground has shifted its attention away from assaults against network perimeters and operating systems in favor of those exploiting application flaws.

Security Wire Daily News

Full Story :
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1195528,00.html

?track=sy160

- **EU issues warning on security**

Governments and businesses must do more to improve IT security if the European Union (EU) is to achieve its goal of becoming the world's leading knowledge economy by 2010.

Andrea Pirotti, executive director of the EU's European Network Information Security Agency (Enisa), says member states and online businesses must work harder to assure users that the internet is a safe place to transact.

Computing

Full Story :
http://www.computing.co.uk/computing/news/2158797/eu-issues-warning-security

New Vulnerabilities Tested in SecureScout

- **13367 Yahoo! Messenger Denial of Service Weakness (Remote File Checking)**

Yahoo! Messenger is a free instant messaging software.

Ivan Ivan has discovered a weakness in Yahoo! Messenger, which potentially can be exploited by malicious people to cause a DoS (Denial of Service).

The weakness is caused due to an error within the handling of certain messages. This can be exploited to crash another user's Yahoo! Messenger client via a specially crafted message that contains a non-ascii character.

Successful exploitation requires that the user has not configured the application to ignore malicious users that are not on his Messenger list.

The weakness has been confirmed in version 7.5.0.814. Other versions may also be affected.

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

References:

Original Advisory:
http://secunia.com/advisories/20773/

Vendor URL:
http://messenger.yahoo.com/

CVE Reference:

- **14728 Mozilla Firefox "js_ValueToFunctionObject()" method, arbitrary code execution (Remote File Checking)**

A vulnerability has been reported in Firefox.

An error in a security check in the "js_ValueToFunctionObject()" method can be exploited to execute arbitrary code via "setTimeout()" and "ForEach".

The vulnerability has been reported in version 1.5.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2006/mfsa2006-28.html

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference:
CVE-2006-1726

❖ 14729 Mozilla Firefox XUL content windows and the history mechanism, arbitrary code execution (Remote File Checking)

A vulnerability has been reported in Firefox.

An error in the interaction between XUL content windows and the history mechanism can be exploited to trick users into interacting with a browser user interface which is not visible.

Successful exploitation may allow execution of arbitrary code.

The vulnerability has been reported in version 1.5.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2006/mfsa2006-29.html

Other references:
MISC: https://bugzilla.mozilla.org/show_bug.cgi?id=327014
BID:17516
URL:http://www.securityfocus.com/bid/17516
FRSIRT:ADV-2006-1356
URL:http://www.frsirt.com/english/advisories/2006/1356
SECUNIA:19631
URL:http://secunia.com/advisories/19631
SECUNIA:19649
URL:http://secunia.com/advisories/19649

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2006-1725

❖ 14730 Mozilla Firefox "RebuildConsideringRows()" error, memory corruption Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

An error in the processing of malformed tables in "RebuildConsideringRows()" can be exploited to cause a memory corruption.

The vulnerability has been reported in version 1.0 and 1.5.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2006/mfsa2006-27.html

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2006-0748

❖ 14731 Mozilla Firefox "View Image" Local Resource Linking Weakness (Remote File Checking)

Eric Foley has discovered a weakness in Firefox, which can be exploited by malicious people to bypass certain security restrictions.

Internet web sites are normally not allowed to link to local resources. It is, however, possible by a malicious web site to open local content in the browser by tricking a user into right-clicking and choosing "View Image" on a broken image, which is referencing a local resource (e.g. via the file: URI handler).

NOTE: This does not pose any direct security impact by itself, but may be exploited in combination with other vulnerabilities.

The weakness has been confirmed in version 1.5.0.2. Other versions may also be affected.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2006/mfsa2006-39.html

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2006-1942

❖ 16276 WinAmp MIDI File Handling Buffer Overflow Vulnerability (Remote File Checking)

BassReFLeX has discovered a vulnerability in WinAmp, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is cause due to a boundary error within the MIDI plug-in (in_midi.dll) when handling MIDI files. This can be exploited to cause a heap-based buffer overflow via a malicious ".mid" file with a specially crafted header.

Successful exploitation may allow execution of arbitrary code.

The vulnerability has been confirmed in version 5.23 and has also been reported in version 5.21. Other versions may also be affected.

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

References:
Original advisory:
http://www.winamp.com/player/version_history.php#5.24
http://www.milw0rm.com/exploits/1935
http://www.fortinet.com/FortiGuardCenter/advisory/FG-2006-16.html

Other references:
http://secunia.com/advisories/20722/

Product homepage:
http://www.winamp.com/

CVE Reference:

❖ 16277 Linux Kernel "xt_sctp" Denial of Service Vulnerability

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

The vulnerability is caused due to missing checks on the SCTP chunk length within the "xt_sctp" code. This may result in an infinite loop that exhausts system resources via a zero chunk length.

The vulnerability has been reported in versions lower than 2.6.17.1.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.17.1

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-3085

❖ 16278 Sendmail Multi-Part MIME Message Handling Denial of Service

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

The vulnerability is cause due to an error in the termination of the recursive "mime8to7()" function when performing MIME conversions. This can be exploited to cause a certain sendmail process to crash when it runs out of stack space while processing a deeply nested malformed MIME message.

Successful exploitation causes the delivery of other queued messages to fail or causes the generated core dump files to fill up available disk space.

The vulnerability has been reported in version 8.13.6 and prior.

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

References:

Original Advisory:
http://www.sendmail.com/security/advisories/SA-200605-01.txt.asc
http://www.fortinet.com/FortiGuardCenter/advisory/FG-2006-18.html

CVE Reference: CVE-2006-1173

❖ 16279 Microsoft Excel Repair Mode Code Execution Vulnerability (Remote File Checking)

A vulnerability has been discovered in Microsoft Excel, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a memory corruption error in the "repair mode" functionality used for repairing corrupted documents. This can be exploited via a specially crafted Excel documents.

Successful exploitation allows execution of arbitrary code.

The vulnerability has been confirmed on a fully updated Windows XP SP2 system with Microsoft Excel 2003 SP2. Other versions may also be affected.

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

References:

Original advisory:
http://www.microsoft.com/technet/security/advisory/921365.mspx
http://blogs.technet.com/msrc/archive/2006/06/16/436174.aspx

Other references:
BUGTRAQ:20060618 Microsoft Excel 0-day Vulnerability FAQ document written

URL:http://www.securityfocus.com/archive/1/archive/1/437636/100/0/threaded
MISC: http://blogs.securiteam.com/?p=451
CONFIRM: http://blogs.technet.com/msrc/archive/2006/06/16/436174.aspx
CERT:TA06-167A
URL:http://www.us-cert.gov/cas/techalerts/TA06-167A.html
MISC: http://isc.sans.org/diary.php?storyid=1420
CERT-VN:VU#802324
URL:http://www.kb.cert.org/vuls/id/802324
BID:18422
URL:http://www.securityfocus.com/bid/18422
FRSIRT:ADV-2006-2361
URL:http://www.frsirt.com/english/advisories/2006/2361
OSVDB:26527
URL:http://www.osvdb.org/26527
SECTRACK:1016316
URL:http://securitytracker.com/id?1016316
SECUNIA:20686
URL:http://secunia.com/advisories/20686
XF:excel-unspecified-code-execution(27179)
URL:http://xforce.iss.net/xforce/xfdb/27179

CVE Reference: CVE-2006-3059

❖ 16280 Microsoft Windows Hyperlink Object Library Buffer Overflow (Remote File Checking)

kcope has discovered a vulnerability in Microsoft Windows, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in hlink.dll within the handling of Hyperlinks in e.g. Excel documents. This can be exploited to cause a stack-based buffer overflow by tricking a user into clicking a specially crafted Hyperlink in a malicious Excel document.

Successful exploitation allows execution of arbitrary code.

The vulnerability has been confirmed on a fully patched Windows XP SP2 system running Microsoft Excel 2003 SP2. Other versions and products using the vulnerable library may also be affected.

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

References:

Original advisory:
http://lists.grok.org.uk/pipermail/full-disclosure/2006-June/047005.html

Other references:
http://blogs.technet.com/msrc/archive/2006/06/20/437826.aspx
http://www.kb.cert.org/vuls/id/394444
* FULLDISC:20060618 ***ULTRALAME*** Microsoft Excel Unicode Overflow
* URL:http://marc.theaimsgroup.com/?l=full-disclosure&m=115067840426070&w=2

* MISC: http://www.milw0rm.com/exploits/1927
* MISC: http://blogs.technet.com/msrc/archive/2006/06/20/437826.aspx
* BID:18500
* URL:http://www.securityfocus.com/bid/18500
* FRSIRT:ADV-2006-2431
* URL:http://www.frsirt.com/english/advisories/2006/2431
* SECUNIA:20748
* URL:http://secunia.com/advisories/20748

CVE Reference: CVE-2006-3086

New Vulnerabilities found this Week

Sendmail Multi-Part MIME Message Handling Denial of Service

"Denial of Service"

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

The vulnerability is cause due to an error in the termination of the recursive "mime8to7()" function when performing MIME conversions. This can be exploited to cause a certain sendmail process to crash when it runs out of stack space while processing a deeply nested malformed MIME message.

Successful exploitation causes the delivery of other queued messages to fail or causes the generated core dump files to fill up available disk space.

The vulnerability has been reported in version 8.13.6 and prior.

References:
http://www.sendmail.org/releases/8.13.7.html
http://www.sendmail.com/security/advisories/SA-200605-01.txt.asc
http://www.kb.cert.org/vuls/id/146718

Microsoft Windows Hyperlink Object Library Buffer Overflow

"Tricking a user into clicking a specially crafted Hyperlink"

kcope has discovered a vulnerability in Microsoft Windows, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in hlink.dll within the handling of Hyperlinks in e.g. Excel documents. This can be exploited to cause a stack-based buffer overflow by tricking a user into clicking a specially crafted Hyperlink in a malicious Excel document.

Successful exploitation allows execution of arbitrary code.

The vulnerability has been confirmed on a fully patched Windows XP SP2 system running Microsoft Excel 2003 SP2. Other versions and products using the vulnerable library may also be affected.

References:

http://blogs.technet.com/msrc/archive/2006/06/20/437826.aspx
http://www.kb.cert.org/vuls/id/394444

Microsoft Excel Repair Mode Code Execution Vulnerability

"Execution of arbitrary code"

A vulnerability has been discovered in Microsoft Excel, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a memory corruption error in the "repair mode" functionality used for repairing corrupted documents. This can be exploited via a specially crafted Excel documents.

Successful exploitation allows execution of arbitrary code.

The vulnerability has been confirmed on a fully updated Windows XP SP2 system with Microsoft Excel 2003 SP2. Other versions may also be affected.

NOTE: This vulnerability is a so-called 0-day and is already being actively exploited.

References:
http://www.microsoft.com/technet/security/advisory/921365.mspx
http://blogs.technet.com/msrc/archive/2006/06/16/436174.aspx

GnuPG "parse-packet.c" Denial of Service Vulnerability

"Denial of Service"

A vulnerability has been reported in GnuPG, which potentially can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is cause due to an input validation error within "parse-packet.c" when handling the length of a message packet. This can be exploited to cause gpg to consume large amount of memory or crash via an overly large packet length in a message packet. This can be further exploited to cause an integer overflow which leads to a possible memory corruption that crashes gpg.

Successful exploitation requires that the "--no-armor" option is used.

The vulnerability has been reported in version 1.4.3 and in development version 1.9.20. Prior versions may also be affected.

References:
http://seclists.org/lists/fulldisclosure/2006/May/0774.html
http://cvs.gnupg.org/cgi-bin/viewcvs.cgi/trunk/g10/parse-packet.c?rev=4157&r1=4141&r2=4157

WinAmp MIDI File Handling Buffer Overflow Vulnerability

"Execution of arbitrary code"

BassReFLeX has discovered a vulnerability in WinAmp, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is cause due to a boundary error within the MIDI plug-in (in_midi.dll) when handling MIDI files. This can be exploited to cause a heap-based buffer overflow via a malicious ".mid" file with a specially crafted header.

Successful exploitation may allow execution of arbitrary code.

The vulnerability has been confirmed in version 5.23 and has also been reported in version 5.21. Other versions may also be affected.

NOTE: The vulnerability may be related to one reported by Fortinet Security Research Team.

References:
http://www.winamp.com/player/version_history.php#5.24

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