netVigilance

ScoutNews Team **July 1, 2005**
Issue # 26

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Tough week for Google; hacker cracks new media service and they get charged with 'click-fraud'. Some gains for us whitehats; Brits collar identity thieves and China cracks down on IP infringement.

Enjoy reading

Call or email netVigilance to get an update on SecureScout.
(503) 524 5758 or sales@netVigilance.com

Top Security News Stories this Week

- **Google releases in-browser video… Hacker releases key to lock**

Less than 24 hours after Google released it's VideoLAN media player; the Norwegian hacker Jon Lech Johansen posted a hack that effectively disables a Google modification to prevent users from playing videos that are not hosted on Google's servers.

The browser plug-in can be downloaded for free from http://video.google.com, and was intended to play content exclusive to Google video. After installing the viewer, users can enter keywords into the search box and the results will show up with still-screen captures and small bits of text next to each

Yahoo news

Related Links :

http://www.pcmag.com/article2/0,1759,1831965,00.asp?kc=PCYH104059TX1B0100580

http://news.yahoo.com/news?tmpl=story&u=/zd/20050628/tc_zd/155004

❖ British National High Tech Crime Unit nabs internet fraud criminals

The crime duo of one American and one British citizen were arrested for perpetrating identity theft using credit card information supplied by an eastern European organized crime ring.

The two were obtaining credit card accounts through duplication and new applications, buying merchandise online then reselling online.

PC Pro UK

Full Story:
http://www.pcpro.co.uk/news/74497/phishing-gang-caught-by-national-hi-tech-crime-unit.html

❖ China shows signs of getting serious about software piracy

The Ministry of Public Security launches massive operation to crack down on intellectual property infringement. This is an encouraging sign to software and movie makers to stem the trend of IP piracy in China.

Redherring

Full Story:
http://www.redherring.com/Article.aspx?a=12588&hed=China+Nabs+2%2c600+For+Piracy&sector=Industries&subsector=SecurityAndDefense

❖ Google faces first 'click-fraud' case

Click Defense of Fort Collins Co. filed suit that claims Google ads are overvalued due to click fraud. The problem of click fraud has become a hot topic recently. Click-fraud can take several forms, the most common include a company official who clicks on competitors' ads, knowing that it costs his competitors money or the publisher of a Web site which runs pay-per-click ads, because the more the ads on his site are clicked on, the more commission money the publisher receive.

infoworld

Full Story:
http://www.infoworld.com/article/05/07/01/HNadgoogle_1.html

New Vulnerabilities Tested in SecureScout

- **13252 RealPlayer (10.5/10.5 Beta/10/8) / RealOne Player (v2/v1) creating local HTML file Vulnerability (Remote File Checking)**

Several vulnerabilities have been reported in RealOne Player, RealPlayer, Helix Player and Rhapsody, which can be exploited by malicious people to overwrite local files or to compromise a user's system.

An unspecified error can be exploited by a malicious web site to create a local HTML file on the user's system and then trigger a RM file that references this local HTML file.

Successful exploitation requires that a user opens a malicious MP3, RealMedia or AVI file, or visits a malicious web site that causes the user's browser to automatically load the malicious file.

The following products are affected:
* RealPlayer 10.5 (6.0.12.1040-1069)
* RealPlayer 10
* RealOne Player v2
* RealOne Player v1
* RealPlayer 8
* RealPlayer Enterprise
* Mac RealPlayer 10 (10.0.0.305 - 331)
* Mac RealOne Player
* Linux RealPlayer 10 (10.0.0 - 4)
* Helix Player (10.0.0 - 4)
* Rhapsody 3 (build 0.815 - 0.1006)

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

References:

Original Advisories:
http://service.real.com/help/faq/security/050623_player/EN/
http://www.service.real.com/help/faq/security/security062305.html
http://www.idefense.com/application/poi/display?id=250&type=vulnerabilities
http://www.eeye.com/html/research/advisories/AD20050623.html

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

CVE Reference: CAN-2005-1766, CAN-2005-2052, CAN-2005-2054, CAN-2005-2055

- **15636 AOL Instant Messenger Font Denial of Service Vulnerability (Remote File Checking)**

The remote host is using AOL Instant Messenger (AIM) - a p2p software, which may not be suitable for a business environment.

A vulnerability exists in AOL Instant Messenger (AIM) which could cause the AIM client to stop responding.

Attacks can be launched if an instant message containing an unusual number of character fonts followed by the '<hr>' HTML comment, is sent and received by an AIM recipient. Restart of the application may be required in order to regain normal functionality.

It should be noted that HTML comments other than '<hr>' could successfully exploit this issue.

In addition, this vulnerability may also affect Netscape's AIM client.

Vulnerable: AOL Instant Messenger 4.7

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

References:

Original advisory:
http://www.securityfocus.com/archive/1/247707
http://www.securityfocus.com/archive/1/218920

Product HomePage:
http://www.aim.com/get_aim/win/latest_win.adp

Other references:
http://www.securityfocus.com/bid/3756

CVE Reference: CAN-2001-1421

❖ **15637 AOL Instant Messenger Long Filename Denial of Service Vulnerability (Remote File Checking)**

The remote host is using AOL Instant Messenger (AIM) - a p2p software, which may not be suitable for a business environment.

A vulnerability exists in AOL Instant Messenger (AIM) which could cause the AIM client to stop responding.

If a file being transferred from one client to another, has an unusually long filename. It is possible for the recipient's AIM client to crash.

Vulnerable: AOL Instant Messenger 4.7

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

References:

Original advisory:
http://www.securityfocus.com/archive/1/247707

http://www.securityfocus.com/archive/1/218920

Product HomePage:
http://www.aim.com/get_aim/win/latest_win.adp

Other references:
http://www.securityfocus.com/bid/3756

CVE Reference: CAN-2001-1420

❖ **15640 AOL Instant Messenger BuddyIcon Buffer Overflow Vulnerability (Remote File Checking)**

The remote host is using AOL Instant Messenger (AIM) - a p2p software, which may not be suitable for a business environment.

AOL Instant Messenger (AIM) is a real time messaging service for users that are on line. When AOL Instant Messenger is installed, by default it configures the system so that the aim: URL protocol connects aim:// urls to the AIM client. There exists a buffer overflow in parsing aim:// URL parameters.

The buffer overflow has to do with the parsing of parameters associated with the "buddyicon" option. The stack overflow will occur If the "Source" parameter, which arguments the buddyicon option, is more than 3000 characters in length. It may be possible to execute arbitrary code. Since this vulnerability manifests itself in an URL, a user needs only to click on the URL (which can be embedded in email, webpages, chatrooms, etc) for the flaw to be exploited.

It should be noted that the victim need only have AIM installed on their machine to be vulnerable. Even if AIM is not running, if a user clicks or otherwise activates a malicious aim:// url, the overflow will occur. Additionally it should be noted that AIM is often included/bundled with Netscape Communicator and possibly other popular software programs.

Successful exploitation of this vulnerability will lead to complete comprimise of the target host.

Vulnerable: AOL Instant Messenger 4.2.1193

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

References:

Original advisory:
http://www.atstake.com/research/advisories/2000/a121200-1.txt
http://www.aol.com/aim/home.html

Product HomePage:
http://www.aim.com/get_aim/win/latest_win.adp

Other references:
http://www.securityfocus.com/bid/2122

CVE Reference: CVE-2000-1094

❖ **13250 RealPlayer (10.5/10.5 Beta/10/8) / RealOne Player (v2/v1) "CRealTextFileFormat::ReadDone()" boundary error (Remote File Checking)**

Several vulnerabilities have been reported in RealOne Player, RealPlayer, Helix Player and Rhapsody, which can be exploited by malicious people to overwrite local files or to compromise a user's system.

A boundary error in the "CRealTextFileFormat::ReadDone()" function when processing RealText streams can be exploited to cause a heap-based buffer overflow via a specially crafted RealMedia file.

Successful exploitation allows execution of arbitrary code.

The following products are affected:
* RealPlayer 10.5 (6.0.12.1040-1069)
* RealPlayer 10
* RealOne Player v2
* RealOne Player v1
* RealPlayer 8
* RealPlayer Enterprise
* Mac RealPlayer 10 (10.0.0.305 - 331)
* Mac RealOne Player
* Linux RealPlayer 10 (10.0.0 - 4)
* Helix Player (10.0.0 - 4)
* Rhapsody 3 (build 0.815 - 0.1006)

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

References:

Original Advisories:
http://service.real.com/help/faq/security/050623_player/EN/
http://www.service.real.com/help/faq/security/security062305.html
http://www.idefense.com/application/poi/display?id=250&type=vulnerabilities
http://www.eeye.com/html/research/advisories/AD20050623.html

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

CVE Reference: CAN-2005-1766, CAN-2005-2052, CAN-2005-2054, CAN-2005-2055

❖ **15641 AOL Instant Messenger 'aim://' Buffer Overflow Vulnerability (Remote File Checking)**

The remote host is using AOL Instant Messenger (AIM) - a p2p software, which may not be suitable for a business environment.

AOL Instant Messenger (AIM) is a real time messaging service for users that are on line. When AOL Instant Messenger is installed, by default it configures the system so that the

aim: URL protocol connects aim:// urls to the AIM client. There exists a buffer overflow in parsing aim:// URL parameters.

This vulnerability exists in versions of AOL Instant previous to Messenger 4.3.2229. By sending a specially crafted URL ,using the 'aim:' protocol, comprised of 'goim' and 'screenname' parameters, it is possible for a remote user to overflow the buffer during a memory copy operation and execute arbitarary code.

It should be noted that the victim need only have AIM installed on their machine to be vulnerable. Even if AIM is not running, if a user clicks or otherwise activates a malicious aim:// url, the overflow will occur. Additionally it should be noted that AIM is often included/bundled with Netscape Communicator and possibly other popular software programs.

Successful exploitation of this vulnerability will lead to complete comprimise of the target host.

Vulnerable: AOL Instant Messenger 4.2.1193

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

References:

Original advisory:
http://www.securityfocus.com/archive/1/151190
http://www.atstake.com/research/advisories/2000/a121200-1.txt

Product HomePage:
http://www.aim.com/get_aim/win/latest_win.adp

Other references:
http://www.securityfocus.com/bid/2118

CVE Reference: XXXXXXXX

❖ **13249 RealPlayer (10.5/10.5 Beta/10/8) / RealOne Player (v2/v1) unspecified error (Remote File Checking)**

Several vulnerabilities have been reported in RealOne Player, RealPlayer, Helix Player and Rhapsody, which can be exploited by malicious people to overwrite local files or to compromise a user's system.

An unspecified error can be exploited to overwrite local files or to execute an ActiveX control on a user's system via a specially crafted MP3 file.

The following products are affected:
* RealPlayer 10.5 (6.0.12.1040-1069)
* RealPlayer 10
* RealOne Player v2
* RealOne Player v1
* RealPlayer 8
* RealPlayer Enterprise
* Mac RealPlayer 10 (10.0.0.305 - 331)
* Mac RealOne Player

* Linux RealPlayer 10 (10.0.0 - 4)
* Helix Player (10.0.0 - 4)
* Rhapsody 3 (build 0.815 - 0.1006)

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

References:

Original Advisories:
http://service.real.com/help/faq/security/050623_player/EN/
http://www.service.real.com/help/faq/security/security062305.html
http://www.idefense.com/application/poi/display?id=250&type=vulnerabilities
http://www.eeye.com/html/research/advisories/AD20050623.html

CVE Reference: CAN-2005-1766, CAN-2005-2052, CAN-2005-2054, CAN-2005-2055

❖ **13251 RealPlayer (10.5/10.5 Beta/10/8) / RealOne Player (v2/v1) processing of AVI movie files boundary error (Remote File Checking)**

Several vulnerabilities have been reported in RealOne Player, RealPlayer, Helix Player and Rhapsody, which can be exploited by malicious people to overwrite local files or to compromise a user's system.

A boundary error in the processing of AVI movie files can be exploited to cause a heap-based buffer overflow via a specially crafted AVI movie file.

Successful exploitation allows execution of arbitrary code.

The following products are affected:
* RealPlayer 10.5 (6.0.12.1040-1069)
* RealPlayer 10
* RealOne Player v2
* RealOne Player v1
* RealPlayer 8
* RealPlayer Enterprise
* Mac RealPlayer 10 (10.0.0.305 - 331)
* Mac RealOne Player
* Linux RealPlayer 10 (10.0.0 - 4)
* Helix Player (10.0.0 - 4)
* Rhapsody 3 (build 0.815 - 0.1006)

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

References:

Original Advisories:
http://service.real.com/help/faq/security/050623_player/EN/
http://www.service.real.com/help/faq/security/security062305.html
http://www.idefense.com/application/poi/display?id=250&type=vulnerabilities
http://www.eeye.com/html/research/advisories/AD20050623.html

CVE Reference: CAN-2005-1766, CAN-2005-2052, CAN-2005-2054, CAN-2005-2055

❖ 15638 AOL Instant Messenger Large BuddyIcon Denial of Service Vulnerability (Remote File Checking)

The remote host is using AOL Instant Messenger (AIM) - a p2p software, which may not be suitable for a business environment.

A vulnerability exists in AOL Instant Messenger (AIM) which could cause the AIM client to stop responding.

AIM does not properly check the size of a user's BuddyIcon when sending instant messages. Therefore, a user with an unusually large BuddyIcon image display dimensions sending instant messages, could cause target clients to stop responding.

Vulnerable: AOL Instant Messenger 4.7

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

References:

Original advisory:
http://www.securityfocus.com/archive/1/247707
http://www.securityfocus.com/archive/1/218920

Product HomePage:
http://www.aim.com/get_aim/win/latest_win.adp

Other references:
http://www.securityfocus.com/bid/3756

CVE Reference: CAN-2001-1417

❖ 15639 AOL Instant Messenger HTML Comments DoS Vulnerability (Remote File Checking)

The remote host is using AOL Instant Messenger (AIM) - a p2p software, which may not be suitable for a business environment.

A vulnerability exists in AOL Instant Messenger (AIM) which could cause the AIM client to stop responding.

Attacks can be launched if an instant message containing an unusual number of HTML comments, is sent and received by an AIM recipient. Restart of the application may be required in order to regain normal functionality. This has also been known to work when using the chat invite message function.

It has been reported that the majority of AOL's versions of AIM is subject to this vulnerability. This reportedly, includes Netscape's AIM client.

Vulnerable: AOL Instant Messenger 4.7.2480

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

References:

Original advisory:
http://www.securityfocus.com/archive/1/247707
http://www.securityfocus.com/archive/1/218255

Product HomePage:
http://www.aim.com/get_aim/win/latest_win.adp

Other references:
http://www.securityfocus.com/bid/3398

CVE Reference: CAN-2001-1419

New Vulnerabilities found this Week

- **Avaya Products TCP Timestamp Denial of Service**
  "Denial of Service"

  Avaya has acknowledged a vulnerability in some products, which can be exploited by malicious people to cause a DoS (Denial of Service) on an active TCP session.

  The vulnerability affect the following products:
  * Avaya G250/G350/G700 (all versions)
  * Avaya Modular Messaging (all versions)
  * Avaya MN100 (versions 1.x through 2)
  * Avaya Intuity LX (versions 1.1 through 5.x)
  * Avaya IP Phones (versions 1.x through 2.1)

  References:
  http://support.avaya.com/elmodocs2/security/ASA-2005-148.pdf
  http://secunia.com/advisories/15393/

- **FreeBSD ipfw Packet Matching Security Issue**
  "Bypass the firewall ruleset"

  A security issue has been reported in FreeBSD, which can be exploited by malicious people to bypass the firewall ruleset.

  The problem is caused due to insufficient concurrency handling in the ipfw tables lookup code. This may lead to the corruption of cached address entries and cause some packets to be incorrectly matched.

  Successful exploitation may allow some packets to pass through the firewall when they should have been dropped.

  The security issue only affects Symmetric Multi-Processor (SMP) systems, or Uni-Processor (UP) systems with the non-default PREEMPTION kernel

option enabled.

References:
ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:13.ipfw.asc

- **FreeBSD TCP Stack Implementation Vulnerabilities**

"Denial of Service"

FreeBSD has issued an update for the TCP stack. This fixes a vulnerability, which can be exploited by malicious people to cause a DoS (Denial of Service) on active TCP sessions.

Additionally, an error has also been fixed, which causes TCP SYN packets to be accepted for established connections making it possible to overwrite certain TCP options.

References:
ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:15.tcp.asc
http://secunia.com/advisories/15393/

- **Cisco IOS RADIUS Authentication Security Bypass**

"Bypass RADIUS authentication"

A vulnerability has been reported in Cisco IOS, which can be exploited by malicious people to bypass RADIUS authentication.

The vulnerability is caused due to an error in the AAA (Authentication, Authorization, and Accounting) RADIUS authentication method making it possible to bypass it by supplying an overly long username.

Successful exploitation bypasses the RADIUS authentication.

The vulnerability only affects devices running the following version of Cisco IOS and configured with a RADIUS authentication and a fallback method to "none" with "local" or no other method in between:
* 12.2T based trains
* 12.3 based trains
* 12.3T based trains
* 12.4 based trains

References:
http://www.cisco.com/warp/public/707/cisco-sa-20050629-aaa.shtml

- **Linux Kernel "syscall()" Argument Handling Denial of Service**

"Denial of Service"

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

The vulnerability is caused due to an error in "fault.c" and can cause the kernel to crash when handling specially crafted "syscall()" arguments on the AMD64 platform when running in 32-bit compatibility mode.

References:
http://www.ubuntulinux.org/support/documentation/usn/usn-143-1

- **RealOne / RealPlayer / Helix Player / Rhapsody Multiple Vulnerabilities**
  "Overwrite local files or to compromise a user's system"

Several vulnerabilities have been reported in RealOne Player, RealPlayer, Helix Player and Rhapsody, which can be exploited by malicious people to overwrite local files or to compromise a user's system.

1) An unspecified error can be exploited to overwrite local files or to execute an ActiveX control on a user's system via a specially crafted MP3 file.

2) A boundary error in the "CRealTextFileFormat::ReadDone()" function when processing RealText streams can be exploited to cause a heap-based buffer overflow via a specially crafted RealMedia file.

Successful exploitation allows execution of arbitrary code.

3) A boundary error in the processing of AVI movie files can be exploited to cause a heap-based buffer overflow via a specially crafted AVI movie file.

Successful exploitation allows execution of arbitrary code.

4) An unspecified error can be exploited by a malicious web site to create a local HTML file on the user's system and then trigger a RM file that references this local HTML file.

Successful exploitation requires that a user opens a malicious MP3, RealMedia or AVI file, or visits a malicious web site that causes the user's browser to automatically load the malicious file.

The following products are affected by some or all of the vulnerabilities:
* RealPlayer 10.5 (6.0.12.1040-1069)
* RealPlayer 10
* RealOne Player v2

* RealOne Player v1
* RealPlayer 8
* RealPlayer Enterprise
* Mac RealPlayer 10 (10.0.0.305 - 331)
* Mac RealOne Player
* Linux RealPlayer 10 (10.0.0 - 4)
* Helix Player (10.0.0 - 4)
* Rhapsody 3 (build 0.815 - 0.1006)

References:
http://service.real.com/help/faq/security/050623_player/EN/
http://www.service.real.com/help/faq/security/security062305.html
http://www.idefense.com/application/poi/display?id=250&type=vulnerabilities
http://www.eeye.com/html/research/advisories/AD20050623.html

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