netVigilance

ScoutNews Team **June 10, 2005**
Issue # 23

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

An Inquiring mind can cause Trojan infection, Balmer speaks out on protecting kids from unfit internet content, Stay Vigilante to prevent becoming a Spam Zombie and Citi Corp. takes a shot at the messenger in their case of sloppy handling of customer data.

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

- **Phony Michael Jackson suicide story used to spread**

Users who click on the link visit a bogus website that attempts to exploit well-known Windows vulnerabilities to install a Trojan called Borobt-Gen onto surfer's PCs.

Keep your anti-virus up-to-date, scan for Vulnerabilities frequently and fight that urge to get gossip via email.

The Register

Full Story :

http://www.theregister.com/2005/06/10/jackson_trojan_spam/

- **Balmer advocates novel concepts of common sense + parental involvement for network security.**

Steve Balmer tells the Associated Press that the huge leaps in convenience brought on by the internet; does not change the fact that parents need to educate their children on right and wrong and avoid visiting those ‘seedier’ corners of the www.

I couldn’t agree more. With all forms of media available today, we all still need to exercise discretion in deciding what we are going to take in. Just because it’s out there, doesn’t mean that I have to partake in it and we can’ t rely on others to completely filter out what they deem unfit for us to have access to.

Associated Press

http://www.newsfactor.com/news/Ballmer-Warns-of-Internet-Dangers/story.xhtml?story_id=02200255ASO2

- **No surprise; Zombies Rise**

The latest numbers on the increase of ‘Zombie’ pc’s; shows a sharp increase from April to May. As you may know; Zombie computers are created by Phishers, Pharmers and Spammers by infecting unsuspecting systems to spread their brand of Malware. In many cases, the user does not even realize that their system is infected.
I’m telling you; scan and scour frequently to keep the malware out.

Red Herring

Related Links:
http://www.redherring.com/Article.aspx?a=12192&hed=Computer+Zombies+on+the+Rise&sector=Industries&subsector=SecurityAndDefense

- **UPS blamed in missing Citi Group customer data**

In the name-and-lay-blame game, Citi points finger at UPS for ‘misplacing’ records of 4 million customers. If I read the data security standards such as GLBA, ISO 17799; the financial institution is responsible for the handling of data and the overseeing of 3rd-party vendors. Was UPS informed of the sensitivity of the data? Was the data ‘lost’ beforehand? Like the Time-Warner / Iron Mtn. fumble; I still hold the financial institution responsible, after all, aren’t they the ones that request and profit from the use of our personal information?

Related Links:
http://news.yahoo.com/news?tmpl=story&cid=568&e=3&u=/nm/financial_citigroup_tapes_dc
http://security.itworld.com/4341/050607citigroup/page_1.html
http://www.chicagotribune.com/technology/chi-0506070278jun07,0,7616859.story?coll=chi-business-hed

New Vulnerabilities Tested in SecureScout

❖ 13236 AOL Instant Messenger Buddy Icon 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.

The running version of AOL Instant Messanger that has is prone to an integer overflow in its GIF parser, 'ateimg32.dll'. Using a specially-crafted GIF file as a buddy icon, an attacker can cause a crash of the affected AIM client and potentially even execute arbitrary code remotely.

Version affected:
AIM 5.9.3797 for Windows 98/ME/2K/XP (5.96 MB) and all prior versions.

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

References:

Original advisory:
http://www.security-protocols.com/modules.php?name=News&file=article&sid=2748

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

Other references:
http://www.nessus.org/plugins/index.php?view=single&id=18432
http://securityfocus.com/bid/13880

CVE Reference: None

❖ 13237 AOL Instant Messenger Buddy Icon Predictable File Location Weakness (Remote File Checking)

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

It has been reported that AOL Instant Messenger stores imported Buddy Icons in a predictable location on client systems that may allow an attacker to facilitate further attacks which could eventually lead to execution of arbitrary code.

This issue has been tested on AOL Instant Messenger versions 4.3 to 5.5, however, it is possible that other versions are affected as well.

Vulnerable: AOL Instant Messenger 5.5.3415 Beta

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

References:

Original advisory:
http://www.securityfocus.com/archive/1/354448

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

Other references:
http://www.securityfocus.com/bid/9698

CVE Reference: None

❖ 13238 AOL Instant Messenger Buddy Icon Warning 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.

AOL Instant Messenger (AIM) is prone to an issue that may allow malicious parties to deny the availability of the service to other users. This issue may permit unauthorized users to abuse the AIM warning system to force other users offline, resulting in a denial of service until the warning level of the user decreases. This issues reportedly allows users to warn arbitrary users if they have a buddy icon.

Last Affected version: AOL Instant Messenger 5.2.3292

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

References:

Original advisory:
http://www.securityfocus.com/archive/1/348094

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

Other references:
http://www.securityfocus.com/bid/9257/info

CVE Reference: None

❖ 13239 AOL Instant Messenger Getfile Screenname Buffer Overrun 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 remotely exploitable buffer overrun vulnerability has been reported in AOL Instant Messenger (AIM). Attackers may exploit this by enticing a user of the client to follow a maliciously constructed AIM URI (using the AIM protocol handler) that performs a "getfile" operation with an overly long value as the screenname.

Vulnerable: AOL Instant Messenger 5.2.3292
Not Vulnerable: AOL Instant Messenger 5.5.3415 Beta

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

References:

Original advisory:
http://www.digitalpranksters.com/advisories/aol/AIMProtocolBO.html
http://www.securityfocus.com/archive/1/

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

Other references:
http://www.securityfocus.com/bid/8825

CVE Reference: None

❖ 13240 AOL Instant Messenger Forced File Download 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 has been discovered in AOL Instant Messenger (AIM), which could allow an attacker to force a user to download an attacker-supplied file.

If a vulnerable user has an option enabled which allows users to download files without a prompt, it may be possible to force the user to download a file. The file will be transfered without prompting the target user for authorization.

Exploiting this issue may allow an attacker to fill a victims hard drive with a file of excessive length.

Vulnerable: AOL Instant Messenger 5.0.2938

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

References:

Original advisory:
http://www.securityfocus.com/archive/1/301277

Product HomePage:

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

Other references:
http://www.securityfocus.com/bid/6259

CVE Reference: None

❖ 13241 AOL Instant Messenger Screen Name 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 is vulnerable to a buffer overflow condition. When viewing the information about a screen name containing 88 characters or longer, AOL Instant Messenger will crash. Although not yet confirmed, arbitrary code execution may be possible.

This vulnerability was discovered in AIM v5.1.3036. It is not yet known whether other versions are affected.

Vulnerable: AOL Instant Messenger 5.1.3036

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

References:

Original advisory:
http://www.securityfocus.com/archive/1/300279
http://www.securityfocus.com/archive/1/300418

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

Other references:
http://www.securityfocus.com/bid/6194

CVE Reference: None

❖ 13242 AOL Instant Messenger Local File Execution 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 prone to an issue which may allow attackers to execute arbitrary files on the client system. It is possible to send a malicious link which references local files to a user of the client. When the link is visited, the referenced file on the client's local filesystem will be executed.

To exploit this issue, the attacker must know the exact location of the file to be executed. Additionally, there can be no spaces in the path or filename. This limits exploitability, since files must be on the same partition and command line arguments cannot be supplied.

Versions other than AOL Instant Messenger 4.8.2790 do not seem to be affected by this vulnerability. The vulnerability was reported for Microsoft Windows versions of the client.

Not Vulnerable: AOL Instant Messenger 5.0.2938

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

References:

Original advisory:
http://www.securityfocus.com/archive/1/296568

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

Other references:
http://www.securityfocus.com/bid/6027

CVE Reference: None

❖ 13243 AOL Instant Messenger Link Special Character Remote Heap 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.

AIM is the AOL Instant Messenger. It is available for various platforms, including Linux and Microsoft Windows. This vulnerability affects the Windows client.

A problem has been reported in the handling of special characters. When an URL is sent to a user containing special characters that must be converted to addressable format, an overflow may occur. This has reportedly been reproduced to create a denial of service.

Vulnerable: AOL Instant Messenger 4.8.2646

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

References:

Original advisory:
http://www.securityfocus.com/archive/1/288980

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

Other references:
http://www.securityfocus.com/bid/5492/info

CVE Reference: None

❖ 13244 AOL Instant Messenger Unauthorized Actions 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.

The AOL Instant Messenger client is prone to an issue which may allow maliciously crafted HTML to perform unauthorized actions (such as adding entries to the buddy list) on behalf of the user of a vulnerable client. This condition is due to how the client handles "aim:" URIs. These actions will be taken without prompting or notifying the user.

This issue was reported for versions of AIM running on Microsoft Windows and MacOS. The Linux version of the client is not affected by this vulnerability.

Not Vulnerable: AOL Instant Messenger 4.8.2616

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

References:

Original advisory:
http://www.securityfocus.com/archive/1/282443

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

Other references:
http://www.securityfocus.com/bid/5246

CVE Reference: None

❖ 13245 AOL Instant Messenger AddBuddy Hyperlink 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 possible buffer overflow vulnerability exists in the AIM. The condition is related to processing of malformed aim:AddBuddy hyperlinks.

If a victim clicks on an AddBuddy hyperlink consisting of many comma delimited screen names, a crash occurs. It is not known if this vulnerability can be exploited to execute arbitrary code.

Vulnerable: AOL Instant Messenger 4.8.2646

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

References:

Original advisory:
http://www.securityfocus.com/archive/1/271976

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

Other references:
http://www.securityfocus.com/bid/4709/info

CVE Reference: CVE-2002-0785

New Vulnerabilities found this Week

- **Linux Kernel "ptrace()" and "mmap()" Vulnerabilities**

  “Denial of Service”

Two vulnerabilities have been reported in the Linux kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service) or potentially gain escalated privileges.

1) Insufficient address validation in "ptrace()" on the AMD64 platform can be exploited to crash the kernel by setting an invalid segment base.

2) An error in the "mmap()" function may result in creation of memory maps with a start address after the end address. This can be exploited to cause a DoS or potentially gain escalated privileges.

References:

http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11.11

http://www.ubuntulinux.org/support/documentation/usn/usn-137-1

- **Mac OS X Security Update Fixes Multiple Vulnerabilities**

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

1) A boundary error in AFP Server within the support for legacy clients can be exploited to cause a buffer overflow.

Successful exploitation allows execution of arbitrary code.

2) A bug in AFP Server when using an ACL-enabled storage volume may in

certain situations result in an ACL remaining attached when a file with POSIX-only permissions is copied.

3) An input validation error can be exploited to access arbitrary files on a Bluetooth-enabled system using directory traversal attacks via the Bluetooth file and object exchange services.

4) A weakness in CoreGraphics can be exploited via a specially crafted PDF document to crash an application using either PDFKit or CoreGraphics to rendor PDF documents.

5) An error in the CoreGraphics Window Server can be exploited by console users to gain escalated privileges by launching commands into a root session.

6) Insecure folder permissions are set on the system's cache folder and Dashboard system widgets.

7) A race condition in the temporary file creation of launchd can be exploited by malicious, local users to take ownership of arbitrary files on the system.

8) An error in LaunchServices can result in file extensions and MIME types marked as unsafe to bypass download safety checks if they're not mapped to an Apple UTI (Uniform Type Identifier).

9) A security issue in MCX Client may disclose Portable Home Directory credentials to local users.

10) A security issue in NFS causes a NFS export restricted using "-network" and "-mask" to be exported to "everyone".

11) Multiple vulnerabilities in PHP can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

12) A boundary error in vpnd can be exploited by malicious, local users to cause a buffer overflow via an overly long Server_id parameter and execute arbitrary code with escalated privileges on systems configured as a VPN server.

References:

http://docs.info.apple.com/article.html?artnum=301742

http://secunia.com/advisories/14792/

- **Mozilla / Mozilla Firefox Frame Injection Vulnerability**
  “Spoof the contents of web sites”

A seven year old vulnerability has been re-introduced in Mozilla and Firefox, which can be exploited by malicious people to spoof the contents of web sites.

The vulnerability has been confirmed in Firefox 1.0.4 and Mozilla 1.7.8. Other versions may also be affected.

References:

http://secunia.com/advisories/11978/

- **GNU Mailutils "sql_escape_string()" SQL Injection Vulnerability**

  "SQL injection attacks"

Primoz Bratanic has reported a vulnerability in GNU Mailutils, which potentially can be exploited by malicious people to conduct SQL injection attacks.

The vulnerability is caused due to an input validation error in the function "sql_escape_string()" in "auth/sql.c" where the backslash character is not properly escaped. This can be exploited to bypass the SQL injection protection and potentially manipulate SQL queries by injecting arbitrary SQL code.

References:

http://security.gentoo.org/glsa/glsa-200506-02.xml

- **Dzip Directory Traversal Vulnerability**

  "Input validation error"

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

The vulnerability is caused due to an input validation error when extracting ".dz" files. This makes it possible to have files extracted to arbitrary locations outside the current directory via directory traversal attacks.

The vulnerability has been confirmed in version 2.9 for Windows. Other versions may also be affected.

References:

http://www.gentoo.org/security/en/glsa/glsa-200506-03.xml

- **Windows Remote Desktop Protocol Private Key Disclosure**

  "Man-in-the-Middle attacks"

Massimiliano Montoro has reported a security issue in Microsoft Windows, which can be exploited by malicious people to conduct MitM (Man-in-the-Middle) attacks.

The problem is that the private key used for signing a terminal server's public key is hard-coded into the mstlsapi.dll library. This can be exploited to calculate a valid signature, which can be used for performing MitM attacks.

Successful exploitation requires that a malicious person is able to intercept traffic between the terminal client and terminal server.

NOTE: Functionality for exploiting this has reportedly been included in Cain & Abel 2.7.

References:

http://www.oxid.it/downloads/rdp-gbu.pdf

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