netVigilance

ScoutNews Team **February 25, 2005**
Issue # 8

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Homeland Security will send you back to school to sharpen your information security skills, Google tells you where to shop. The Brits will wake you up with the latest cyber attacks and network security shows no signs of slowing.

Enjoy and 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

- **Dept of Homeland Security and the National Science Foundation partner to foster Cyber- Security education programs.**

To meet the increasing demand for knowledgeable computer security professionals; Homeland Security; through the Scholarship for Service (SFS) program, will fund colleges and universities to award 2-year scholarships in computer security and information assurance.

US-CERT

Full Story: http://www.us-cert.gov/press_room/schlrshp_srvce.html

❖ Google AutoLink : Is resistance futile?

Google introduces AutoLink feature in their Internet Explorer toolbar in version 3. (Firefox not supported.) This tool will automatically convert certain web contents such as US addresses, Package Tracking Numbers, ISBNs, and Vehicle Identification Numbers into urls.

Controversy is brewing over this 'feature' for various reasons. First of all, Google will determine which vendors get the automatic reference, essentially Adware in a different wrapper. Secondly, Google (and hackers) will be altering clients (your browser) in order to add the link information.

Related Links:
http://www.addict3d.org/index.php?page=viewarticle&type=security&ID=3366
http://www.freedom-to-tinker.com/archives/000772.html

❖ UK Government announces free Virus alert service

The UK Government announced that it will provide free virus alert service; ITsafe, run by the National Infrastructure Security Co-ordination Centre (NISCC).

The low-volume alert service will deliver messages on computer virus' deemed the most serious by the agency. These messages can be delivered by email and mobile phone text messaging services.

This is a great compliment to SecureScout. Alerts of an impending attack will be a prompt for you to update your testcase database and immediately scan the affected systems for vulnerabilities.

❖ Network Security Industry strong; 28% growth in 2004.

Industry tops $4Billion, strongest growth was seen in Hybrid Solutions, IDS/IPS, and SSL VPN. Growth is estimated to continue driven by the need to address the ever-increasing number and severity of computer security threats.

Full Story:

http://press.arrivenet.com/tec/article.php/595062.html

New Vulnerabilities Tested in SecureScout

- **13196 The remote host is using Gaim - a p2p software, which may not be suitable for a business environment**

The remote host is using Gaim - a p2p software,
which may not be suitable for a business environment

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

References: http://gaim.sourceforge.net/

CVE Reference: CAN-2005-0472 CAN-2005-0473

- **14701 bitlance winter has discovered a weakness in Internet Explorer, which can be exploited by malicious people to conduct phishing attacks**

Windows XP SP2 has a security feature, which forces the URL of a popup to the present in the title bar when a popup has been opened without the address bar.

The problem is that the title bar can be spoofed via an overly long hostname. This can e.g. be exploited by a malicious web site to trick a user into entering sensitive information in a popup placed over a trusted site.

The weakness has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP2.

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

References:
http://secunia.com/advisories/14335/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0500

CVE Reference: CAN-2005-0500

- **15164 Secunia Research has discovered a vulnerability in Yahoo! Messenger, which can be exploited by malicious people to trick users into executing malicious files.**

Secunia Research has discovered a vulnerability in Yahoo! Messenger, which can be exploited by malicious people to trick users into executing malicious files.

The problem is that files with long filenames are not displayed correctly in the file transfer dialogs. This can be exploited to trick users into accepting and potentially executing malicious files.

Successful exploitation requires that the option "Hide extension for known file types" is enabled in Windows (default setting).

The vulnerability has been confirmed in version 6.0.0.1750. Other versions may also be affected.

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

References:

Secunia Research:
http://secunia.com/secunia_research/2005-2/advisory/

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

CVE Reference: CAN-2005-0243

- **15165 Secunia Research has discovered a vulnerability in Yahoo! Messenger, which can be exploited by malicious, local users to gain escalated privileges.**

Yahoo! Messenger is a free instant messaging software.

The vulnerability is caused due to a combination of weak default directory permissions and the Audio Setup Wizard (asw.dll) invoking the "ping.exe" utility insecurely during the connection testing phase. This can be exploited to execute arbitrary code with the privileges of another user by placing a malicious "ping.exe" file in the application's "Messenger" directory.

Successful exploitation requires that a user runs the Audio Setup Wizard and that the application has been installed in a non-default location (not as a subdirectory to the "Program Files" directory).

The vulnerability has been confirmed in version 6.0.0.1750 for Windows. Other versions may also be affected.

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

References:

Original Advisory:

Secunia Research:

http://secunia.com/secunia_research/2004-6/

Yahoo! Inc:

http://messenger.yahoo.com/security/update6.html

Vendor URL:

http://messenger.yahoo.com/

CVE Reference: CAN-2005-0242

- **15493 An off-by-one boundary error in the mailbox handling can be exploited by malicious, authenticated users to cause a buffer overflow.**

Cyrus Imapd server is a common implementation of the IMAP4 protocol that is use mainly on unix servers.

An off-by-one boundary error in the imapd annotate extension can be exploited by malicious, authenticated users to cause a buffer overflow.

An unspecified boundary error in fetchnews can be exploited by peer news admins to cause a stack-based buffer overflow.

An unspecified boundary error in backend can be exploited by malicious administrative users to cause a stack-based buffer overflow.

An unspecified boundary error in imapd can be exploited by malicious users on certain platforms to cause a stack-based buffer overflow.

Successful exploitation may allow execution of arbitrary code.

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

References:
http://asg.web.cmu.edu/archive/message.php?mailbox=archive.info-cyrus&msg=33723
http://secunia.com/advisories/14383/
http://asg.web.cmu.edu/cyrus/download/

CVE Reference: none**.**

- **15918 Cirpian Radu has reported a security issue with an unknown impact in ArGoSoft FTP Server.**

ArGoSoft FTP Server is an FTP server for Windows95/98/NT.

The problem is that shortcut files (.lnk) can be copied with the "SITE COPY" command.

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

References:
http://secunia.com/advisories/14372/
http://www.argosoft.com/applications/ftpserver/

CVE Reference: none.

❖ **16004 Remus Hociota has reported a vulnerability in ArGoSoft FTP Server, which can be exploited by malicious users to bypass certain security restrictions.**

ArGoSoft FTP Server is an FTP server for Windows95/98/NT.

The vulnerability is caused due to an error in the validation of shortcut (.lnk) files extracted from ZIP files via the "SITE UNZIP" command and can be exploited to access restricted resources.

Successful exploitation requires that "SITE UNZIP" command support is enabled.

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

References:
http://secunia.com/advisories/14172/
http://www.argosoft.com/applications/ftpserver/

CVE Reference: none.

❖ **16005 Two vulnerabilities have been reported in ArGoSoft FTP Server, where one can be exploited by malicious people to enumerate valid usernames and the other has an unknown impact.**

ArGoSoft FTP Server is an FTP server for Windows95/98/NT.

Two vulnerabilities have been reported in ArGoSoft FTP Server, where one can be exploited by malicious people to enumerate valid usernames and the other has an unknown impact.

1) The "USER" command returns a 530 error response if the username does not exists.

2) It is possible to upload shortcut (".lnk") files.

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

References:

Original Advisory:

http://www.lovebug.org/argosoft_advisory.txt

Vendor URL:

http://www.argosoft.com/applications/ftpserver/

CVE Reference: none.

- **16006 STORM has discovered multiple vulnerabilities in ArGoSoft FTP Server, which can be exploited by malicious users to determine the existence of files, cause a DoS (Denial of Service), or compromise a vulnerable system.**

ArGoSoft FTP Server is an FTP server for Windows95/98/NT.

1) Boundary errors within the handling of arguments supplied to the "SITE ZIP" and "SITE COPY" FTP commands can be exploited to cause buffer overflows. This may potentially allow execution of arbitrary code with the privileges of the FTP server.

2) An input validation error within the handling of arguments supplied to the "SITE UNZIP" FTP command may disclose the presence of arbitrary files on an affected system. This can be exploited via a parameter containing the "../" character sequence.

3) An error within the argument handling for the "SITE PASS" FTP command can be exploited to corrupt the user database by supplying an overly long password string.

The vulnerabilities have been reported version 1.4.1.5 and prior.

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

References:

Original Advisory:

http://secunia.com/advisories/11002/

Vendor URL:

http://www.argosoft.com/applications/ftpserver/

CVE Reference: none.

- **16007 A vulnerability has been reported in ArGoSoft FTP Server, which can be exploited by malicious users to cause a DoS (Denial of Service).**

ArGoSoft FTP Server is an FTP server for Windows95/98/NT.

The vulnerability is caused due to a boundary error when handling input supplied to the "XCWD" FTP command. This can be exploited by supplying an overly long argument (more than 4096 characters), which causes a buffer overflow.

Successful exploitation has been reported to crash the service. However, execution of arbitrary code may potentially also be possible, though this has not been confirmed.

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

References:

CVE Reference:

Original Advisory:

http://secunia.com/advisories/9864/

Vendor URL:

http://www.argosoft.com/applications/ftpserver/

New Vulnerabilities found this Week

- **Cyrus IMAP Server Buffer Overflow Vulnerabilities**
  "Buffer Overflow"

Some vulnerabilities have been reported in Cyrus IMAP Server, which potentially can be exploited by malicious people to compromise a vulnerable system.

1) An off-by-one boundary error in the mailbox handling can be exploited by malicious, authenticated users to cause a buffer overflow.

2) An off-by-one boundary error in the imapd annotate extension can be exploited by malicious, authenticated users to cause a buffer overflow.

3) An unspecified boundary error in fetchnews can be exploited by peer news admins to cause a stack-based buffer overflow.

4) An unspecified boundary error in backend can be exploited by malicious administrative users to cause a stack-based buffer overflow.

5) An unspecified boundary error in imapd can be exploited by malicious users on certain platforms to cause a stack-based buffer overflow.

Successful exploitation may allow execution of arbitrary code.

References:
http://asg.web.cmu.edu/archive/message.php?mailbox=archive.info-cyrus&msg=33723
http://secunia.com/advisories/14383/

- **phpMyAdmin Local File Inclusion and Cross-Site Scripting**
  "Cross-site scripting attacks and disclose sensitive information"

Maksymilian Arciemowicz has reported some vulnerabilities in phpMyAdmin, which can be exploited by malicious people to conduct cross-site scripting attacks and disclose sensitive information.

1) Input passed to the "strServer", "cfg[BgcolorOne]", and "strServerChoice" parameters in "select_server.lib.php", the "bgcolor" and "row_no" parameters in "display_tbl_links.lib.php", the "left_font_family" parameter in "theme_left.css.php", and the "right_font_family" parameter in "theme_right.css.php" is not properly sanitised before being returned to users. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

Successful exploitation requires that "register_globals" is enabled.

2) Input passed to the "GLOBALS[cfg][ThemePath]" parameter in "phpmyadmin.css.php" and "cfg[Server][extension]" parameter in "database_interface.lib.php" is not properly verified before being used to include files. This can be exploited to include arbitrary files from local resources.

Successful exploitation requires that "register_globals" is enabled and that "magic_quotes_gpc" is disabled.

The vulnerabilities have been reported in version 2.6.1. Other versions may also be affected.

It is also possible to disclose the full path to certain scripts by accessing them directly.

References:
http://sourceforge.net/tracker/index.php?func=detail&aid=1149383&group_id=23067&atid=377408

- **Gaim Two Denial of Service Weaknesses**
  "Denial of Service"

Two weaknesses have been reported in Gaim, which can be exploited by malicious people to cause a DoS (Denial of Service).

1) An error within the parsing of received SNAC packets can be exploited to cause a user's Gaim application to become unresponsive when receiving specially crafted packets.

2) An error within the processing of HTML can be exploited to crash the application when receiving specially crafted HTML.

References:
http://gaim.sourceforge.net/security/index.php?id=10
http://gaim.sourceforge.net/security/index.php?id=11
http://www.kb.cert.org/vuls/id/523888
http://www.kb.cert.org/vuls/id/839280

- **Yahoo! Messenger File Transfer Filename Spoofing**
  "Trick users into executing malicious files"

Secunia Research has discovered a vulnerability in Yahoo! Messenger, which can be exploited by malicious people to trick users into executing malicious files.

The problem is that files with long filenames are not displayed correctly in the file transfer dialogs. This can be exploited to trick users into accepting and potentially executing malicious files.

Successful exploitation requires that the option "Hide extension for known file types" is enabled in Windows (default setting).

The vulnerability has been confirmed in version 6.0.0.1750. Other versions may also be affected.

References:
http://secunia.com/secunia_research/2005-2/advisory/

❖ **Yahoo! Messenger Audio Setup Wizard Privilege Escalation**
"Gain escalated privileges"

Secunia Research has discovered a vulnerability in Yahoo! Messenger, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to a combination of weak default directory permissions and the Audio Setup Wizard (asw.dll) invoking the "ping.exe" utility insecurely during the connection testing phase. This can be exploited to execute arbitrary code with the privileges of another user by placing a malicious "ping.exe" file in the application's "Messenger" directory.

Successful exploitation requires that a user runs the Audio Setup Wizard and that the application has been installed in a non-default location (not as a subdirectory to the "Program Files" directory).

The vulnerability has been confirmed in version 6.0.0.1750 for Windows. Other versions may also be affected.

References:
http://secunia.com/secunia_research/2004-6/

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.