netVigilance

ScoutNews Team **February 18, 2005**
Issue # 7

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

MyDoom sneaks back into systems disguised in wrapper, Government agencies are getting 'left behind' on the lessons of information security and the Cabir is here; knocking out Blue Teeth in mobile devices and automobiles?

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

- **Sneaky new 'MyDoom' variant goes undetected by anti-virus software.**

The new variant is based on an older MyDoom virus but is packaged in a wrapper that allows it to not be detected by anti-virus software. The WORM was detected on Wednesday, and is quickly circling the globe.

Apparently, this new strain, propagates itself through it's own SMTP mailer. It scans your hard drive; picking off email addresses that you have stored, then mails itself to them. Some vendors have reported this as W32/Bofra. The characteristics of the WORM are as follows:

- Spoofed From address
- A Subject line containing one of the following:
    - Hi!
    - <blank>
    - <random characters>
    - Confirmation
    - funny photos :)
    - hello
    - hey!
- Body text containing a URL that leads to a malicious site.

It is recommended that you update all anti-virus, Vulnerability Assessment packages to protect yourself.

US-CERT

References:

http://www.us-cert.gov/current/current_activity.html#w32/mydoom

http://www.us-cert.gov/other_sources/viruses.html

❖ Federal Agency report cards are in; congressional watchdog committee gives D+

Representative Tom Davis (R-Va.) http://tomdavis.org/ chairman of the House Government Reform Committee, identified several areas where improvements are needed including; testing of contingency plans, configuration management, incident reporting, and specialized training for employees with security responsibilities.

The report also uncovers a lack of efficiency in improving information security within government agencies. The fact that the scores have not made marked improvements in an environment that is becoming increasingly more hostile; raises concern of an impending disaster as a result well orchestrated cyber attack against these agencies.

IDG News Service

Full Story:
http://www.nwfusion.com/news/2005/0216usagenc.html

- **First cases of Cabir mobile virus found in US.**

As you read in ScoutNews issue #6; February 11th, 2005; there is an increased threat of mobile virus' infecting portable devices, automobiles and other appliances. They're here!

The first cases of the Cabir virus was discovered in two cell phone in a window display of a Santa Monica, Ca. store. The infected phones may have been infecting Bluetooth capable devices of passersby's.

The Cabir virus targets popular mobile operating systems; destroying files, dial 900 numbers or 911, and made them crumble under denial-of-service attacks.

In a related story, Lexus responds to blogger to debuke rumors that Bluetooth capable navigation systems in their cars are susceptible to the Cadir Virus.
Webpronews.com

http://www.webpronews.com/news/ebusinessnews/wpn-45-20050218LexusTalkstoaBlogtoSquashVirusRumors.html

New Vulnerabilities Tested in SecureScout

- **14699 Mozilla and Firefox are reported prone to a security vulnerability that could allow a malicious website to bypass drag-and-drop functionality security policies.**

Mozilla and Firefox are reported prone to a security vulnerability that could allow a malicious website to bypass drag-and-drop functionality security policies.

It is demonstrated that it is possible to exploit this vulnerability with an image

that renders correctly in the Firefox browser but that, when dragged and dropped onto the local file system, will be saved with a '.bat' file extension.

Because the batch file interpreter on Microsoft Windows is particularly lenient when it comes to syntax, batch commands appended to the image file will be executed if the image that was dragged and dropped is invoked.

The vulnerabilities have been confirmed in Mozilla 1.7.5 and Firefox 1.0. Other versions may also be affected.

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

References:

Original Advisory:
http://securityfocus.com/archive/1/389654
http://www.mikx.de/index.php?p=8

Other References:
http://secunia.com/advisories/14160/
https://bugzilla.mozilla.org/show_bug.cgi?id=280947

Product HomePage:
http://www.mozilla.org/products/mozilla1.x/

CVE Reference:

- **14700 Secunia Research has discovered a weakness in Sun Java Plugin, allowing malicious web sites to write arbitrary content to a file with a predictable name.**

The problem is that the plugin creates temporary files for class files using a file name which becomes predictable when referenced using the old 8dot3 file schema (FAT16/DOS support).

The temporary file creation in itself is not a vulnerability and should not pose any risk to the system. However, combined with certain Microsoft Internet Explorer functionality and vulnerabilities this can be exploited to compromise a vulnerable system.

The weakness has been confirmed in version 1.5.0 (build 1.5.0_01-b08). Other versions may also be affected.

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

References:

Original Advisory:

http://secunia.com/secunia_research/2004-7/advisory/

Other References:
US-CERT VU#544392:
http://www.kb.cert.org/vuls/id/544392
http://secunia.com/advisories/11070/

Product HomePage:
http://java.sun.com/j2se/

CVE Reference: none.

- **15140 vulnerabilities have been reported in Adobe Reader and Adobe Acrobat, which can be exploited by malicious people to disclose sensitive information or compromise a user's system**

1) A format string error within the eBook plug-in when parsing ".etd" files can be exploited to execute arbitrary code via a specially crafted eBook containing format specifiers in the "title" and "baseurl" fields.

2) Multiple vulnerabilities in libpng have been acknowledged, which can be exploited by malicious people to compromise a vulnerable system.

3) An error within the handling of Flash files embedded in PDF documents can be exploited to read the content of files on a user's system.

The vulnerabilities have been reported in versions 6.0.0 through 6.0.2.

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

References:
http://www.adobe.com/support/downloads/detail.jsp?ftpID=2679

CVE Reference: CAN-2004-0597, CAN-2004-1153

- **15161 Mozilla and Firefox are reported prone to a cross-domain script execution vulnerability.**

The issue is reported to exist because the browsers fail to prevent JavaScript that originates from one tab from accessing properties of a site contained in another tab. Typically, the Javascript security manager prevents a 'javascript:' URI from one domain to be opened in the context of a site from another window, however tabbed browsing can be used to bypass this security restriction.

This issue is reported to affect Firefox 1.0, however, it is possible that other versions are affected as well. Mozilla 1.7.5 was also reported vulnerable.

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

References:

Original Advisory:
http://securityfocus.com/archive/1/389658
http://www.mikx.de/index.php?p=9

Other References:
http://secunia.com/advisories/14160/

Product HomePage:
http://www.mozilla.org/products/mozilla1.x/
http://www.mozilla.org/products/firefox/

CVE Reference: CAN-2005-0231

- **15162 A remote configuration manipulation vulnerability affects Mozilla and Firefox.**

This issue is due to a failure of the application to properly secure sensitive configuration scripts from being activated by remote attackers.

An attacker may leverage this issue to alter an unsuspecting user's configuration settings; this may lead to a false sense of security as sensitive settings may be manipulated without the user's knowledge.

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

References:

Original Advisory:
http://securityfocus.com/archive/1/389657
http://www.mikx.de/index.php?p=10

Other References:
http://secunia.com/advisories/14160/

Product HomePage:
http://www.mozilla.org/products/mozilla1.x/
http://www.mozilla.org/products/firefox/

CVE Reference: CAN-2005-0232

❖ **15163 Mozilla and Firefox are reported prone to vulnerabilities that surround the handling of International Domain Names.**

The vulnerabilities exist due to inconsistencies in how International Domain Names are processed. Reports indicate that this inconsistency can be leveraged to spoof address bar, status-bar, and SSL certificate values.

These vulnerabilities may be exploited by a remote attacker to aid in phishing style attacks. This may result in the voluntary disclosure of sensitive information to a malicious website due to a false sense of trust.

Although these vulnerabilities are reported to affect Web browsers, mail clients that depend on the Web browser to generate HTML code may also be affected.

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

References:

Original Advisory:
http://securityfocus.com/archive/1/389695
http://www.shmoo.com/idn/homograph.txt

Secunia online test:
http://secunia.com/multiple_browsers_idn_spoofing_test/

Other References:
http://secunia.com/advisories/14163/
http://securityfocus.com/bid/12461/

Product HomePage:
http://www.mozilla.org/products/mozilla1.x/
http://www.mozilla.org/products/firefox/

CVE Reference:

❖ **15615 Dr_insane has discovered three vulnerabilities in ArGoSoft Mail Server, which can be exploited by malicious people to cause a DoS (Denial of Service), disclose sensitive information, and create arbitrary directories on a vulnerable system.**

1) Input passed to the username in "addnewuser" isn't properly sanitised before being used to create directories. This can be exploited to create a directory in an arbitrary location via directory traversal attacks.

2) An error in the handling of long passwords (about 800 bytes) in "addnewuser" can be exploited to cause a vulnerable service to consume a

large amount of CPU resources.

3) The problem is that the script "viewlogs.pl" can be accessed without any authentication. This can be exploited to disclose some potentially sensitive logging information.

The vulnerabilities have been confirmed in version 1.8.7.4. Other versions may also be affected.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Medium** Risk: **Denial of Service**

References:

http://www.argosoft.com/mailserver/default.aspx

http://secunia.com/advisories/14221/

CVE Reference: none

- **15616 Tan Chew Keong has reported some vulnerabilities in ArGoSoft Mail Server, which can be exploited by malicious users to disclose and manipulate sensitive information, and potentially compromise a user's system.**

1) An input validation error in the attachment handling can be exploited to create or overwrite arbitrary files via directory traversal attacks.

2) The problem is that the "_msgatt.rec" file, which holds information about uploaded files, can be overwritten by an uploaded attachment. This can be exploited to include arbitrary files as attachments in an mail via directory traversal attacks.

3) Input passed to the "Folder" parameter in "msg", "delete", "folderdelete" and "folderadd" isn't properly sanitised before being used. This can be exploited to access or delete mails for other currently logged on users, and create or delete arbitrary directories via directory traversal attacks.

The vulnerabilities have been reported in version 1.8.7.3 and prior.

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

References:

http://www.argosoft.com/mailserver/default.aspx

http://secunia.com/advisories/14161/

CVE Reference: CAN-2005-0367

❖ **15617 Dr_insane has discovered three vulnerabilities in ArGoSoft Mail Server, which can be exploited by malicious people to cause a DoS (Denial of Service), disclose sensitive information, and create arbitrary directories on a vulnerable system.**

1) Input passed to the username in "addnewuser" isn't properly sanitised before being used to create directories. This can be exploited to create a directory in an arbitrary location via directory traversal attacks.

2) An error in the handling of long passwords (about 800 bytes) in "addnewuser" can be exploited to cause a vulnerable service to consume a large amount of CPU resources.

3) The problem is that the script "viewlogs.pl" can be accessed without any authentication. This can be exploited to disclose some potentially sensitive logging information.

The vulnerabilities have been confirmed in version 1.8.7.4. Other versions may also be affected.

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

References:
http://www.argosoft.com/mailserver/default.aspx
http://secunia.com/advisories/14221/

CVE Reference: none.

❖ **15618 Tan Chew Keong has reported some vulnerabilities in ArGoSoft Mail Server, which can be exploited by malicious users to disclose and manipulate sensitive information, and potentially compromise a user's system.**

1) An input validation error in the attachment handling can be exploited to create or overwrite arbitrary files via directory traversal attacks.

2) The problem is that the "_msgatt.rec" file, which holds information about uploaded files, can be overwritten by an uploaded attachment. This can be exploited to include arbitrary files as attachments in an mail via directory traversal attacks.

3) Input passed to the "Folder" parameter in "msg", "delete", "folderdelete" and "folderadd" isn't properly sanitised before being used. This can be exploited to access or delete mails for other currently logged on users, and create or delete arbitrary directories via directory traversal attacks.

The vulnerabilities have been reported in version 1.8.7.3 and prior.

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

References:
http://www.argosoft.com/mailserver/default.aspx
http://secunia.com/advisories/14161/

CVE Reference: CAN-2005-0367

New Vulnerabilities found this Week

- **Linux Kernel Multiple Vulnerabilities**

  "Gain knowledge of potentially sensitive information, Denial of Service, bypass certain security restrictions"

  Some vulnerabilities have been reported in the Linux kernel. These can be exploited by malicious, local users to gain knowledge of potentially sensitive information or cause a DoS (Denial of Service), or by malicious people to cause a DoS or bypass certain security restrictions.

  1) Insufficient permission checking in the "shmctl()" function allows any process to lock/unlock arbitrary System V shared memory segments that fall within the RLIMIT_MEMLOCK limit.

  This can be exploited to unlock locked memory of other processes, which may result in sensitive information being written to swap space.

  2) A race condition exists in the terminal handling of the "setsid()" function used for starting new process sessions.

  3) Table sizes in "nls_ascii.c" are incorrectly set to 128 instead of 256, which may be exploited to cause buffer overflows and crash the kernel.

  4) A design error in the netfilter/iptables module can be exploited to crash the kernel or bypass firewall rules via specially crafted packets.

  References:
  http://www.ubuntulinux.org/support/documentation/usn/usn-82-1

- **VMware Workstation gdk-pixbuf Path Searching Vulnerability**

  "Gain escalated privileges"

Tavis Ormandy has discovered a vulnerability in VMware Workstation, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to VMware Workstation searching for gdk-pixbuf modules in a world-writable directory. This can be exploited via a malicious module to execute arbitrary code with the privileges of the user running VMware Workstation.

Successful exploitation requires that gdk-pixbuf is not installed on the system.

The vulnerability has been confirmed in version 4.5.2 (build 8848). Other versions may also be affected.

References:

http://www.gentoo.org/security/en/glsa/glsa-200502-18.xml

- **PHP-Nuke Cross-Site Scripting Vulnerabilities**

"Conduct cross-site scripting attacks"

Janek Vind "waraxe" has reported two vulnerabilities in PHP-Nuke, which can be exploited by malicious people to conduct cross-site scripting attacks.

Some input isn't properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site.

The vulnerabilities have been reported in version 6.x through 7.6. Other versions may also be affected.

References:
http://www.waraxe.us/advisory-40.html

- **Sun Solaris FTP Server PASV Commands Denial of Service**

"Denial of Service"

Sun has acknowledged an older vulnerability in Sun Solaris, which can be exploited by malicious users to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the FTP server and can be exploited to consume all available ports on the system by issuing multiple PASV commands.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-57725-1

- **Linux Kernel Memory Disclosure and Privilege Escalation**

"Disclose kernel memory, Gain escalated privileges"

Some vulnerabilities have been reported in the Linux Kernel, which potentially can be exploited by malicious, local users to disclose kernel memory or gain escalated privileges.

1) A race condition in the radeon driver can potentially be exploited to gain escalated privileges.

Successful exploitation reportedly requires DRI (Direct Rendering Infrastructure) privileges on the Radeon hardware.

2) A boundary error in the i2c-viapro driver can be exploited to cause a buffer overflow during a SMBus block read and may allow execution of arbitrary code with escalated privileges.

Successful exploitation depends on the permissions set on the i2c device files and specific hardware combinations.

3) A signedness error in "/proc" can be exploited to cause a buffer overflow when the "locks_read_proc()" function is called with certain arguments.

The vulnerability has been reported in versions 2.6.10 and 2.6.11rc1-bk6 on the i386 architecture. Other versions may also be affected.

4) A signedness error in "drivers/char/n_tty.c" when copying data from kernel space into user space can be exploited to disclose kernel memory.

The vulnerability has been reported in versions 2.6.10 and 2.6.11rc1 on the i386 architecture. Other versions may also be affected.

5) Some potential errors have been reported in the "atm_get_addr()" function in "net/atm/addr.c" and in the "reiserfs_copy_from_user_to_file_region()" function in "fs/reiserfs/file.c".

References:
http://www.guninski.com/where_do_you_want_billg_to_go_today_3.html
http://kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.11-rc4

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