netVigilance

ScoutNews Team

August 19, 2005
Issue # 33

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Zotob: around the world in three days, iPods turn out to be hiding place for illicit data, DHS increases focus on cyber security, vicious infection from Swedish website and AOL data thief does time.

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

❖ **Zotob returns, shuts down production at auto plant, reeks havoc on new agencies**

Production at 13 of DaimlerChrysler's U.S. plants was interrupted this week when Windows 2000 systems fell victim to a Zotob Worm.

A few notable news agencies were also severely affected by the Worm including ABC, CNN, The Associated Press, *The New York Times* and Caterpillar Inc. In California, San Diego County.

Zotob spreads via internet connections as opposed to email or IM attachments, so the outbreak is predicted to fairly mild. with most of the damage occurring in the US, reported outbreaks in Europe and Asia were substantially fewer.

Related Links:
http://www.kmov.com/localnews/stories/kmov_localnews_050819_chryslerworm.8c72c72f.html
http://www.abc.net.au/pm/content/2005/s1441027.htm
http://www.wired.com/news/technology/0,1282,68552,00.html?tw=wn_4techhead

- ### iPods used to hide digital crime data

Law enforcement officials have recently discovered cases where criminals are using iPod mp3 players to store more than criminally-tasteful music.

It seems that the crooks have found a way to hide forged sale documents, bogus bank statements, child pornography and other incriminating materials on the miniature music players.

There is talk that portable mp3 players can be used as malware vehicles; bypassing commonplace network security measures.
redherring

Full Story :

http://www.newhousenews.com/archive/mccutcheon081605.html

- ### Cyber-terrorism becomes focus

DHS is creating a national cyberspace response system to help private sector companies detect and prevent cyber attacks. The chief concern is the nation's vital infrastructure of power, water, waste and dams.

Richard Clarke, a former terrorism and cyber-security czar in the Bush administration was quoted: "People downplay the importance of cyber-security, claiming that no one will ever die in a cyber-attack, but they're wrong, this is a serious threat."
Source

Full Story:
http://ww.pennnet.com/news/display_news_story.cfm?Section=WIREN&Category=HOME&NewsID=123541

- ### Swedish website contains malware for visitors

Websense reports that a Swedish website actually contains malware built in that allows hackers to gain complete control of PCs visiting the infected site. The flaw exploits unpatched versions of Internet Explorer. Microsoft released patch last week that removes the vulnerability.
NewsFactor Network

Full Story:
http://www.newsfactor.com/news/Hackers-Exploit-New-Windows-Flaw/story.xhtml?story_id=100009QO6K1O

- ### Former AOL employee sentenced for theft of email addresses

The former AOL employee that sold 92 million screen names and e-mail addresses to spammers was sentenced Wednesday to a year and three months in prison. 25 year old Jason Smathers appeared remorseful at the sentencing, regretting his becoming an

Outlaw.
Associated Press

Full Story:
http://biz.yahoo.com/ap/050817/aol_spamming.html?.v=4

New Vulnerabilities Tested in SecureScout

❖ 13273 Oracle Database Server - Oracle HTTP Server (mod_access) component Unspecified error (jul-2005/DB12)

An unspecified error in the Oracle HTTP Server (mod_access) component can potentially be exploited to disclose or manipulate information.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujul2005.html

Product Homepage:
http://www.oracle.com/

CVE Reference: None

❖ 13275 MySQL multiple crashes Vulnerabilities

Some vulnerabilities have been reported in MySQL, which can be exploited by malicious users to cause a DoS (Denial of Service), or potentially by malicious people to execute arbitrary code.

It is possible for malicious users to crash the server in various ways. See the vendor advisory for details.

Versions of MySQL 4.x up to and including 4.1.12 are vulnerable

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

References:

Original advisories:
http://dev.mysql.com/doc/mysql/en/news-4-1-13.html

Other references:
http://secunia.com/advisories/16170/
http://secunia.com/SA15949/

Vendor:
http://www.mysql.com/

CVE Reference: CAN-2005-2096

❖ 15659 AOL Instant Messenger Password Encryption 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 uses a weak method of encryption while negotiating its sign on process.

The first FLAP packets sent to the OSCAR logon server contain the user login password and screen name which are encrypted using a weak XOR method that is trivial to decrypt.

Vulnerable: AOL Instant Messenger 1.2

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

References:

Original advisory:
http://www.securityfocus.com/bid/6777

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

CVE Reference: None

❖ 15664 Firefox handling of DOM node names Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox, which can be exploited by malicious people to bypass certain security restrictions, conduct cross-site scripting attacks, and compromise a user's system.

An error in the handling of DOM node names with different namespaces can be exploited to execute arbitrary script code with escalated privileges via a specially crafted XHTML document.

Successful exploitation allows execution of arbitrary code.

This vulnerability affects versions up to and including 1.0.4.

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

References:

Original advisory:
http://www.mozilla.org/security/announce/mfsa2005-55.html

Other references:
http://secunia.com/advisories/14938/

http://secunia.com/advisories/16043/

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

CVE Reference: CAN-2005-2260, CAN-2005-2261, CAN-2005-2262, CAN-2005-2263, CAN-2005-2264, CAN-2005-2265, CAN-2005-2267, CAN-2005-2269, CAN-2005-2270

❖ 15665 Firefox insecure cloning of base objects Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox, which can be exploited by malicious people to bypass certain security restrictions, conduct cross-site scripting attacks, and compromise a user's system.

An error caused due to insecure cloning of base objects can be exploited to execute arbitrary script code with escalated privileges.

This vulnerability affects versions up to and including 1.0.4.

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

References:

Original advisory:
http://www.mozilla.org/security/announce/mfsa2005-56.html

Other references:
http://secunia.com/advisories/14938/
http://secunia.com/advisories/16043/

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

CVE Reference: CAN-2005-2260, CAN-2005-2261, CAN-2005-2262, CAN-2005-2263, CAN-2005-2264, CAN-2005-2265, CAN-2005-2267, CAN-2005-2269, CAN-2005-2270

❖ 15666 Firefox Property Manipulation Cross-Site Scripting Vulnerability (Remote File Checking)

Secunia Research has discovered a vulnerability in Firefox, which can be exploited by malicious people to conduct cross-site scripting attacks.

The problem is that the "frames", "parent", "self", and "top" DHTML properties are not properly protected from being modified by another site via JavaScript. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an arbitrary site, which calls a method in one of the modified properties.

The vulnerability has been confirmed in version 1.0.4. Prior versions may also be affected.

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

References:

Original advisory:
http://secunia.com/secunia_research/2005-15/advisory/
http://www.mozilla.org/security/announce/mfsa2005-52.html

Other references:
http://secunia.com/advisories/15549/

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

CVE Reference: CAN-2005-2266

❖ 15671 Mozilla Thunderbird insecure cloning of base objects Vulnerability (Remote File Checking)

Some vulnerabilities have been reported in Thunderbird, which can be exploited by malicious people to bypass certain security restrictions, gain knowledge of potentially sensitive information, conduct cross-site scripting attacks and compromise a user's system.

An error caused due to insecure cloning of base objects can be exploited to execute arbitrary script code with escalated privileges.

Versions up to and including version 1.0.4 are vulnerable.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/mfsa2005-56.html

Other references:
http://secunia.com/advisories/16062/
http://secunia.com/advisories/14820/
http://secunia.com/advisories/15549/

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

CVE Reference: CAN-2005-0989, CAN-2005-1159, CAN-2005-1160, CAN-2005-2261, CAN-2005-2265, CAN-2005-2266, CAN-2005-2269, CAN-2005-2270

❖ 15672 Mozilla Thunderbird privileged UI code Vulnerability (Remote File Checking)

Some vulnerabilities have been reported in Thunderbird, which can be exploited by malicious people to bypass certain security restrictions, gain knowledge of potentially sensitive information, conduct cross-site scripting attacks and compromise a user's system.

Some errors, where certain privileged UI code does not properly validate DOM nodes from the content window, can be exploited to execute arbitrary code.

Successful exploitation may require some user interaction.

Versions up to and including version 1.0.4 are vulnerable.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/mfsa2005-44.html

Other references:
http://secunia.com/advisories/16062/
http://secunia.com/advisories/14820/
http://secunia.com/advisories/15549/

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

CVE Reference: CAN-2005-0989, CAN-2005-1159, CAN-2005-1160, CAN-2005-2261, CAN-2005-2265, CAN-2005-2266, CAN-2005-2269, CAN-2005-2270

❖ 15673 Mozilla Thunderbird input validation errors Vulnerability (Remote File Checking)

Some vulnerabilities have been reported in Thunderbird, which can be exploited by malicious people to bypass certain security restrictions, gain knowledge of potentially sensitive information, conduct cross-site scripting attacks and compromise a user's system.

Some input validation errors when handling parameters of invalid types passed to certain "InstallTrigger" and "XPInstall" related objects via JavaScript may be exploited to execute arbitrary code.

Versions up to and including version 1.0.4 are vulnerable.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/mfsa2005-40.html

Other references:
http://secunia.com/advisories/16062/
http://secunia.com/advisories/14820/
http://secunia.com/advisories/15549/

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

CVE Reference: CAN-2005-0989, CAN-2005-1159, CAN-2005-1160, CAN-2005-2261, CAN-2005-2265, CAN-2005-2266, CAN-2005-2269, CAN-2005-2270

- ❖ **15674 Mozilla Thunderbird JavaScript engine Vulnerability (Remote File Checking)**

Some vulnerabilities have been reported in Thunderbird, which can be exploited by malicious people to bypass certain security restrictions, gain knowledge of potentially sensitive information, conduct cross-site scripting attacks and compromise a user's system.

An error in the JavaScript engine, as a "lambda" replace exposes arbitrary amounts of heap memory after the end of a JavaScript string, may be exploited to disclose sensitive information in memory.

Versions up to and including version 1.0.4 are vulnerable.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/mfsa2005-33.html

Other references:
http://secunia.com/advisories/16062/
http://secunia.com/advisories/14820/
http://secunia.com/advisories/15549/

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

CVE Reference: CAN-2005-0989, CAN-2005-1159, CAN-2005-1160, CAN-2005-2261, CAN-2005-2265, CAN-2005-2266, CAN-2005-2269, CAN-2005-2270

New Vulnerabilities found this Week

- ❖ **Microsoft Design Tools msdds.dll Code Execution Vulnerability**
  “Execute arbitrary code”

A vulnerability has been reported in Microsoft Visual Studio .NET, which potentially can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an error when the "msdds.dll" (Microsoft Design Tools - Diagram Surface) COM object is instantiated in the Internet Explorer browser.

Successful exploitation may allow execution of arbitrary code, but requires that a user is tricked into visiting a malicious web site.

The COM object is known to be installed as part of the following products:
* Microsoft Visual Studio .NET 2003
* Microsoft Office Professional 2003
* Microsoft Office XP

Other products may also include the affected COM object.

NOTE: An exploit has been published. However, there are currently conflicting reports about the exploitability of this issue. Some reports confirm that code execution is possible, while other reports indicate that the problem can't be reproduced. Secunia has currently not been able to reproduce the vulnerability in version 7.10.3077.0 of the COM object.

References:
http://isc.sans.org/diary.php?date=2005-08-18

❖ **Adobe Acrobat / Reader Plug-in Buffer Overflow Vulnerability**
"Execute arbitrary code"

A vulnerability has been reported in Adobe Reader and Adobe Acrobat, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an unspecified boundary error in the core application plug-in and can be exploited to cause a buffer overflow when a specially crafted file is opened.

Successful exploitation may allow execution of arbitrary code.

References:
http://www.adobe.com/support/techdocs/321644.html
http://www.kb.cert.org/vuls/id/896220

❖ **Mac OS X Security Update Fixes Multiple Vulnerabilities**
"Conduct cross-site scripting attacks; Denial of Service; Execution of arbitrary code"

Apple has issued a security update for Mac OS X, which fixes more than 40 vulnerabilities.

1) A boundary error in htdigest can be exploited to cause a buffer overflow by passing an overly long realm argument.

NOTE: htdigest is by default only locally accessible and not setuid / setgid.

2) Two vulnerabilities in Apache 2 can be exploited by malicious people to bypass certain security restrictions or cause a DoS (Denial of Service).

3) A security issue in Apache 2 results in access to ".DS_Store" files and files starting with ".ht" not being fully blocked. The problem is that the Apache configuration blocks access in a case sensitive way, but the Apple HFS+ filesystem performs file access in a case insensitive way.

4) A security issue in Apache 2 makes it possible to bypass the normal Apache file handlers and retrieve file data and resource fork content via HTTP. The problem is that the Apple HFS+ filesystem permits files to have multiple data streams.

NOTE: This issue may also affect other products installed on the HFS+ filesystem.

5) A boundary error in the AppKit component can be exploited to cause a buffer overflow and execute arbitrary code on a user's system when a specially crafted rich text file is opened.

6) A boundary error in the AppKit component can be exploited to cause a buffer overflow and execute arbitrary code on a user's system when a specially crafted Microsoft Word .doc file is opened in e.g. TextEdit.

7) An error in the AppKit component allows malicious, local users with physical access to create additional local accounts.

8) A bug in the System Profiler causes it to display misleading information about whether or not a Bluetooth device requires authentication.

9) A boundary error in the CoreFoundation framework when processing command line arguments can be exploited to cause a buffer overflow and execute arbitrary code.

10) An error in the CoreFoundation framework when parsing Gregorian date information can cause applications to stall.

11) Errors in the CUPS printing service can cause it to stop printing when handling multiple, simultaneous print jobs.

12) A boundary error in Directory Services during the authentication handling can be exploited to cause a buffer overflow and execute arbitrary code.

13) Various errors in the privileged tool dsidentity can be exploited by unprivileged users to add or remove identity user accounts in Directory Services.

14) The slpd program in Directory Services creates temporary files insecurely. This can be exploited via symlink attacks to overwrite arbitrary files with root privileges.

15) An error in HItoolbox may allow VoiceOver services to read contents from secure input fields.

16) An error in Kerberos can potentially be exploited by malicious users to compromise a vulnerable system.

17) Multiple boundary errors in Kerberos can be exploited by malicious people to cause a DoS or potentially compromise a vulnerable system.

18) An error in Kerberos when Kerberos authentication is enabled in addition to LDAP can be exploited to gain access to the root Terminal window.

19) An error in loginwindow can be exploited by malicious users with knowledge of two passwords to access other logged-in accounts when "Fast User Switching" is enabled without knowing these passwords.

20) The Mail component loads remote images in HTML emails (even with this disabled in the user's preferences), which can be exploited to enumerate valid email addresses.

21) Various errors in MySQL can potentially be exploited by malicious users to compromise a vulnerable system and by malicious, local users to perform certain actions on a vulnerable system with escalated privileges.

22) Three vulnerabilities in OpenSSL can be exploited by malicious people to cause a DoS (Denial-of-Service).

23) An unspecified boundary error in the ping utility can be exploited to cause a buffer overflow and potentially gain escalated privileges.

24) An error in QuartzComposerScreenSaver can be exploited by malicious people with physical access to open web pages while the RSS Visualizer screen saver is locked.

25) An error in Safari can be exploited to bypass the normal browser security checks and execute arbitrary commands when a link in a specially crafted rich text file is clicked.

26) A security issue in Safari when submitting forms on a XSL formatted page may cause the information to be submitted to the next visited web page.

27) A security issue in the SecurityInterface component may cause recently used passwords to be visible in the password assistant.

28) A boundary error in servermgrd during the authentication process can be exploited to cause a buffer overflow and execute arbitrary code.

29) A security issue in servermgr_ipfilter may cause certain firewall policies created with the Server Admin tool to not be written to the Active Rules.

30) Some vulnerabilities in Squirrelmail can be exploited to conduct cross-site scripting attacks or disclose and manipulate sensitive information.

31) A boundary error in the traceroute utility can be exploited to cause a buffer overflow and execute arbitrary code.

32) An error in WebKit can be exploited to bypass normal browser security checks and execute arbitrary commands when a link in a specially crafted PDF document is clicked.

33) Various errors in Weblog Server can be exploited to conduct cross-site scripting attacks.

34) A vulnerability in X11 can potentially be exploited by malicious people to compromise a vulnerable system.

35) Errors in zlib can be exploited by malicious people to conduct a DoS against a vulnerable application or potentially to execute arbitrary code.

References:
http://docs.info.apple.com/article.html?artnum=302163

- **PHPTB "absolutepath" Arbitrary File Inclusion Vulnerability**
  "Execution of arbitrary code"

Filip Groszynski has discovered a vulnerability in PHPTB, which can be exploited by malicious people to compromise a vulnerable system.

Input passed to the "absolutepath" parameter in various scripts is not properly verified before being used to include files. This can be exploited to include arbitrary files from local and remote resources.

Example:
http://[host]/classes/admin_o.php?absolutepath=[file]

Successful exploitation requires that "register_globals" is enabled.

The vulnerability has been confirmed in version 2.0. Other versions may also be affected.

References:
http://secunia.com/advisories/16492/

- **ezUpload "path" Arbitrary File Inclusion Vulnerability**
  "Execute arbitrary code"

Johnnie Walker has reported a vulnerability in ezUpload, which can be exploited by malicious people to compromise a vulnerable system.

Input passed to the "path" parameter in various scripts is not properly verified before being used to include files. This can be exploited to include arbitrary files from local and remote resources.

The vulnerability has been reported in version 2.2. Other versions may also be affected.

References:
http://secunia.com/advisories/16434/

- **CPAINT Ajax Toolkit Command Execution Vulnerabilities**
  "Execute arbitrary code"

Thor Larholm has reported some vulnerabilities in CPAINT, which can be exploited by malicious people to conduct cross-site scripting attacks or compromise a vulnerable system.

1) Input passed to the "cpaint_argument[]" parameter is not properly sanitised before being executed. This can be exploited to execute arbitrary code on the server by concatenation of the arguments.

2) The "checkBlacklist()" function in cpaint.inc.asp does not check for the presence of "ExecuteGlobal" and "GetRef" statements. This can be exploited for code execution.

The vulnerabilities have been reported in version 1.3-SP. Prior versions may also be affected.

References:
http://secunia.com/advisories/16454/

- ### phpPgAds & phpAdsNew Multiple Vulnerabilities
  “SQL Injection”

Some vulnerabilities have been reported in phpPgAds and phpAdsNew, which can be exploited by malicious people to disclose certain sensitive information, conduct SQL injection attacks or compromise a vulnerable system.

1) A vulnerable version of XML-RPC for PHP was used.

2) Input passed to the "clientid" parameter in lib-view-direct.inc.php isn't properly sanitised before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.

Successful exploitation requires MySQL 4.1+ or PostgreSQL.

3) Input passed to certain parameters is not properly verified before being used to include files. This can be exploited to include arbitrary local files.

References:
http://secunia.com/advisories/16431/

- ### Multiple XML-RPC for PHP Nested XML Tags PHP Code Execution
  “Execute arbitrary code”

Stefan Esser has reported a vulnerability in XML-RPC, which can be exploited by malicious people to compromise a vulnerable system.

Certain XML tags that are nested in parsed documents are not properly sanitised before being used in an "eval()" call. This can be exploited to execute arbitrary PHP code on a vulnerable system.

The vulnerability has been reported in versions 1.1.1 and prior.

Related vulnerabilities:
PEAR XML_RPC Nested XML Tags PHP Code Execution
XML-RPC for PHP Nested XML Tags PHP Code Execution
eGroupWare XML-RPC Nested XML Tags PHP Code Execution
Nucleus CMS XML-RPC Nested XML Tags PHP Code Execution
MailWatch for MailScanner XML-RPC PHP Code Execution
phpMyFAQ XML-RPC Nested XML Tags PHP Code Execution

References:
http://www.hardened-php.net/advisory_152005.67.html
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2498

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