netVigilance

ScoutNews Team **February 24, 2006**
2006 Issue # 8

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Google fixes big AdWords flaw, Nigerian national get time for last years ChoicePoint ID theft and Microsoft spills Vista versions.

Enjoy reading

Top Security News Stories this Week

- ### Google fixes AdWords XSS vulnerability

Google announced Tuesday that it has patched a vulnerability on it's Adwords website that opened users to a Cross-Site Scripting (XSS) attack. The flaw was uncovered by Finjan Software about 1 month ago and reported to Google.

Google AdWords account holders can configure AdWords to perform a Message Transfer Agent (MTA) that does not require encryption. Hackers could exploit such vulnerabilities to download malicious code on a visitors PC or redirect the user to a phoney website and phish for passwords and other vital data.

Silicon.com

Full Story :

http://software.silicon.com/security/0,39024655,39153194,00.htm

❖ Nigerian national sentenced in ChoicePoint ID theft case

A 42-year old Nigerian national by the name of Olatunji Oluwatosin, was sentenced to 10 years in prison and $6.5 million for his involvement in the infamous ChoicePoint identity theft. Mr. Oluwatosin was apparently serving a 16 month prison sentence for a separate cyber crime.

Wired

Full Story :
http://www.hackinthebox.org/modules.php?op=modload&name=News&file=article&sid=19306

❖ Microsoft posts Vista versions by accident

Up to eight versions of the upcoming Vista operating system were posted to a Microsoft website. The Redmond giant has since removed the binaries but has tipped it's hand a bit in revealing versions including Windows Starter 2007, Windows Vista Business, Windows Vista Enterprise, Windows Vista Home Basic, Windows Vista Home Premium, and Windows Vista Ultimate.

RedHerring

Related Links :
http://www.redherring.com/Article.aspx?a=15835&hed=Vista+Versions+Leaked&sector=Industries&subsector=Computing

New Vulnerabilities Tested in SecureScout

❖ 13353 Oracle Database Server - XML Database component Unspecified error (jan-2006/DB29)

An unspecified error in the XML Database component can potentially be exploited to gain knowledge of certain information, overwrite arbitrary files, and to conduct SQL injection attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html

Other references:
http://www.kb.cert.org/vuls/id/891644
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0272
* MISC:http://www.argeniss.com/research/ARGENISS-ADV-010601.txt
* MISC:http://www.integrigy.com/info/IntegrigySecurityAnalysis-CPU0106.pdf
* MISC:http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html
* CERT:TA06-018A
* URL:http://www.us-cert.gov/cas/techalerts/TA06-018A.html
* CERT-VN:VU#545804
* URL:http://www.kb.cert.org/vuls/id/545804
* CERT-VN:VU#891644
* URL:http://www.kb.cert.org/vuls/id/891644
* BID:16287
* URL:http://www.securityfocus.com/bid/16287
* FRSIRT:ADV-2006-0243
* URL:http://www.frsirt.com/english/advisories/2006/0243
* FRSIRT:ADV-2006-0323
* URL:http://www.frsirt.com/english/advisories/2006/0323
* SECTRACK:1015499
* URL:http://securitytracker.com/id?1015499
* SECUNIA:18493
* URL:http://secunia.com/advisories/18493
* SECUNIA:18608
* URL:http://secunia.com/advisories/18608

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

CVE Reference: CVE-2006-0272

❖ 16130 Winamp ID3v2 Tag Handling Buffer Overflow Vulnerability (Remote File Checking)

Leon Juranic has reported a vulnerability in Winamp, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the handling of ID3v2 tags and can be exploited to cause a buffer overflow via e.g. a MP3 file containing an overly long string in the "Artist" field.

Successful exploitation allows execution of arbitrary code, but requires some user interaction (e.g. that the user adds a malicious MP3 file to a playlist and then plays the file).

The vulnerability has been reported in versions 5.03a, 5.09, and 5.091. Other versions may also be affected.

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

References:

Original advisory:

http://security.lss.hr/en/index.php?page=details&ID=LSS-2005-07-14

Other references:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2310
* BID:14276
* URL:http://www.securityfocus.com/bid/14276
* SECTRACK:1014483
* URL:http://securitytracker.com/id?1014483
* SECUNIA:16077
* URL:http://secunia.com/advisories/16077

Product homepage:
http://www.winamp.com/

CVE Reference: CAN-2005-2310

❖ 16131 Winamp handling of filenames including a UNC path with a long computer name Vulnerability (Remote File Checking)

A boundary error during the handling of filenames including a UNC path with a long computer name can be exploited to cause a buffer overflow via a specially crafted playlist containing a filename with an overly long computer name (about 1040 bytes).

An exploit is publicly available.

The vulnerability has been confirmed in version 5.12. Other versions may also be affected.

Successful exploitation of the vulnerability allows execution of arbitrary code on a user's system when e.g. a malicious website is visited.

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

References:

Original advisory:

http://milw0rm.com/id.php?id=1458

Other references:

http://secunia.com/advisories/18649/

Product homepage:

http://www.winamp.com/

CVE Reference: None

❖ 16132 Winamp boundary error within the parsing of playlists (.m3u or .pls) Vulnerability (Remote File Checking)

A boundary error within the parsing of playlists (.m3u or .pls) can be exploited to cause a stack-based buffer overflow via a playlist containing an overly long, specially crafted filename.

The vulnerability has been reported in version 5.11 and does reportedly not affect prior versions.

Successful exploitation of the vulnerability allows execution of arbitrary code on a user's system when e.g. a malicious website is visited.

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

References:

Original advisory:
http://www.idefense.com/intelligence/vulnerabilities/display.php?id=377

Other references:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0476
* BUGTRAQ:20060130 Winamp 5.12 - 0day exploit - code execution through playlist
* URL:http://www.securityfocus.com/archive/1/423436/100/0/threaded
* MISC:http://milw0rm.com/id.php?id=1458
* MISC:http://www.heise.de/newsticker/meldung/68981
* MISC:http://www.winamp.com/player/version_history.php
* BUGTRAQ:20060131 Re: Re: Winamp 5.12 - 0day exploit - code execution through playlist
* URL:http://www.securityfocus.com/archive/1/archive/1/423548/100/0/threaded
* CERT:TA06-032A
* URL:http://www.us-cert.gov/cas/techalerts/TA06-032A.html
* CERT-VN:VU#604745
* URL:http://www.kb.cert.org/vuls/id/604745
* BID:16410
* URL:http://www.securityfocus.com/bid/16410
* FRSIRT:ADV-2006-0361
* URL:http://www.frsirt.com/english/advisories/2006/0361
* OSVDB:22789
* URL:http://www.osvdb.org/22789
* SECTRACK:1015552
* URL:http://securitytracker.com/id?1015552
* SECUNIA:18649
* URL:http://secunia.com/advisories/18649
* XF:winamp-playlist-computername-bo(24361)
* URL:http://xforce.iss.net/xforce/xfdb/24361

Product homepage:
http://www.winamp.com/

CVE Reference: CVE-2006-0476

❖ 16133 Winamp boundary error within the parsing of playlists containing a filename with a .wma extension Vulnerability (Remote File Checking)

A boundary error within the parsing of playlists containing a filename with a .wma extension can be exploited to cause a buffer overflow via a specially crafted playlist.

The vulnerability has been reported in version 5.094. Other versions may also be affected.

Successful exploitation of the vulnerability allows execution of arbitrary code on a user's system when e.g. a malicious website is visited.

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

References:

Original advisory:
http://www.idefense.com/intelligence/vulnerabilities/display.php?id=378

Other references:
http://secunia.com/advisories/18649/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3188
* BID:16462
* URL:http://www.securityfocus.com/bid/16462
* SECTRACK:1015565
* URL:http://securitytracker.com/id?1015565
* XF:winamp-wma-ext-bo(24417)
* URL:http://xforce.iss.net/xforce/xfdb/24417

Product homepage:
http://www.winamp.com/

CVE Reference: CVE-2005-3188

❖ 16134 Winamp boundary error during the handling of files with an .m3u file extension Vulnerability (Remote File Checking)

A boundary error during the handling of files with an .m3u file extension can be exploited to cause a buffer overflow via a specially crafted playlist containing a file with an overly long filename.

Successful exploitation crashes the application. Arbitrary code execution may be possible, but has not been proven.

The weaknesses have been reported in version 5.13. Prior versions may also be affected.

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

References:

Original advisory:
http://forums.winamp.com/showthread.php?s=&threadid=238648

Other references:

http://secunia.com/advisories/18848/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0708

Product homepage:
http://www.winamp.com/

CVE Reference: CAN-2006-0708

❖ 16135 Winamp boundary error during the handling of overly long filenames Vulnerability (Remote File Checking)

A boundary error during the handling of overly long filenames can be exploited to cause a buffer overflow via a playlist containing a file with an overly long filename.

Successful exploitation crashes the application. Arbitrary code execution may be possible, but has not been proven.

The weaknesses have been reported in version 5.13. Prior versions may also be affected.

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

References:

Original advisory:
http://forums.winamp.com/showthread.php?s=&threadid=238648

Other references:
http://secunia.com/advisories/18848/
http://secway.org/advisory/AD20060216.txt
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0708

Product homepage:
http://www.winamp.com/

CVE Reference: CAN-2006-0708

❖ 16136 Winamp boundary error within the .m3u playlist file handling Vulnerability (Remote File Checking)

A boundary error within the .m3u playlist file handling can be exploited to cause a buffer overflow via a specially crafted .m3u playlist when playing is paused or stopped.

Successful exploitation crashes the application and may reportedly also allow execution of arbitrary code.

The vulnerability has been reported in versions 5.12 and 5.13. Prior versions may also be affected.

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

References:

Original advisory:
http://forums.winamp.com/showthread.php?s=&threadid=238648

Other references:
http://secunia.com/advisories/18848/
http://www.nsfocus.com/english/homepage/research/0601.htm
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0720

Product homepage:
http://www.winamp.com/

CVE Reference: CVE-2006-0720

❖ 16137 Mozilla Firefox errors in the JavaScript engine Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

Some errors in the JavaScript engine where certain temporary variables are not properly protected may be exploited to execute arbitrary code via a user-defined method triggering garbage collection.

The vulnerability affects version 1.5 and prior.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/mfsa2006-01.html

Other references:
* CONFIRM:https://bugzilla.mozilla.org/show_bug.cgi?id=316885
* FEDORA:FEDORA-2006-075
* URL:http://www.redhat.com/archives/fedora-announce-list/2006-February/msg00005.html
* FEDORA:FEDORA-2006-076
* URL:http://www.redhat.com/archives/fedora-announce-list/2006-February/msg00006.html
* MANDRIVA:MDKSA-2006:036
* URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:036
* REDHAT:RHSA-2006:0199
* URL:http://www.redhat.com/support/errata/RHSA-2006-0199.html
* REDHAT:RHSA-2006:0200
* URL:http://www.redhat.com/support/errata/RHSA-2006-0200.html
* BID:16476
* URL:http://www.securityfocus.com/bid/16476
* FRSIRT:ADV-2006-0413
* URL:http://www.frsirt.com/english/advisories/2006/0413
* SECTRACK:1015570
* URL:http://securitytracker.com/id?1015570

* SECUNIA:18700
* URL:http://secunia.com/advisories/18700
* SECUNIA:18703
* URL:http://secunia.com/advisories/18703
* SECUNIA:18704
* URL:http://secunia.com/advisories/18704
* SECUNIA:18708
* URL:http://secunia.com/advisories/18708
* SECUNIA:18709
* URL:http://secunia.com/advisories/18709
* SECUNIA:18705
* URL:http://secunia.com/advisories/18705
* SECUNIA:18706
* URL:http://secunia.com/advisories/18706
* XF:mozilla-javascript-memory-corruption(24430)
* URL:http://xforce.iss.net/xforce/xfdb/24430
* CONFIRM:http://www.mozilla.org/security/announce/mfsa2006-01.html
* CONFIRM:https://bugzilla.mozilla.org/show_bug.cgi?id=322045
* BID:16476
* URL:http://www.securityfocus.com/bid/16476
* FRSIRT:ADV-2006-0413
* URL:http://www.frsirt.com/english/advisories/2006/0413
* SECTRACK:1015570
* URL:http://securitytracker.com/id?1015570
* SECUNIA:18700
* URL:http://secunia.com/advisories/18700
* SECUNIA:18704
* URL:http://secunia.com/advisories/18704
* XF:mozilla-javascript-memory-corruption(24430)
* URL:http://xforce.iss.net/xforce/xfdb/24430

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

CVE Reference: CVE-2006-0292,CVE-2006-0293

❖ 16138 Mozilla Firefox error in the dynamic style handling Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

An error in the dynamic style handling can be exploited to reference freed memory by changing the style of an element from "position:relative" to "position:static".

Successful exploitation may allow execution of arbitrary code.

The vulnerability has been reported in version 1.5.

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

References:

Original Advisories:

http://www.mozilla.org/security/announce/mfsa2006-02.html

Other references:
* CONFIRM:https://bugzilla.mozilla.org/show_bug.cgi?id=317934
* BID:16476
* URL:http://www.securityfocus.com/bid/16476
* FRSIRT:ADV-2006-0413
* URL:http://www.frsirt.com/english/advisories/2006/0413
* SECTRACK:1015570
* URL:http://securitytracker.com/id?1015570
* SECUNIA:18700
* URL:http://secunia.com/advisories/18700
* SECUNIA:18704
* URL:http://secunia.com/advisories/18704

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

CVE Reference: CVE-2006-0294

New Vulnerabilities found this Week

Mac OS X File Association Meta Data Shell Script Execution
“Executing a malicious shell script”

Michael Lehn has discovered a vulnerability in Mac OS X, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an error in the processing of file association meta data in ZIP archives (stored in the "__MACOSX" folder) and mail messages (defined via the AppleDouble MIME format). This can be exploited to trick users into executing a malicious shell script renamed to a safe file extension stored in a ZIP archive or in a mail attachment.

This can also be exploited automatically via the Safari browser when visiting a malicious web site.

The vulnerability has been confirmed on a fully patched system with Safari 2.0.3 (417.8), Mail 2.0.5 (746/746.2), and Mac OS X 10.4.5.

References:
http://www.kb.cert.org/vuls/id/999708

SquirrelMail Cross-Site Scripting and IMAP Injection Vulnerabilities
“Cross-site scripting attacks”

Some vulnerabilities have been reported in SquirrelMail, which can be exploited by malicious users to manipulate certain information and by malicious people to conduct cross-site scripting attacks.

1) Input passed to the "right_main" parameter in "webmail.php" isn't properly sanitised 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 an affected site.

2) Input passed to comments in styles isn't properly sanitised 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 an affected site.

Successful exploitation requires that the user views the malicious data with the Microsoft Internet Explorer browser.

3) Input passed to the "sqimap_mailbox_select mailbox" parameter isn't properly sanitised before being used in a IMAP query and can be exploited to inject arbitrary IMAP commands.

The vulnerabilities have been reported in version 1.4.5 and prior.

References:
http://www.squirrelmail.org/security/issue/2006-02-01
http://www.squirrelmail.org/security/issue/2006-02-10
http://www.squirrelmail.org/security/issue/2006-02-15

Bugzilla Multiple Vulnerabilities
“SQL injection attacks; disclose sensitive information”

Some vulnerabilities have been reported in Bugzilla, which can be exploited by malicious users to conduct SQL injection attacks, and by malicious people to disclose sensitive information and conduct script insertion attacks.

1) Input passed to the "whinedays" parameter in "editparams.cgi" 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 administrative privileges.

The vulnerability has been reported in versions prior to 2.20.1 and 2.22rc1 (from version 2.17.1).

2) The problem is that some RSS readers decode encoded HTML in feed titles. This can be exploited to inject arbitrary HTML and script code, which will be executed in a user's RSS readers session in context of an affected site when the malicious user data is viewed.

The vulnerability has been reported in versions 2.20rc1 through 2.20 and 2.21.1.

3) The problem is that users may send login requests to an incorrect web site when the URL contains a double slash in the path name.

Successful exploitation requires that the login page is a subdirectory of the web root and that the subdirectory is a resolvable address on the user's network.

The vulnerability has been reported in versions prior to 2.20.1 and 2.22rc1 (from version 2.19.3).

References:
http://www.bugzilla.org/security/2.18.4/

PHP-Nuke "Your_Account" Module SQL Injection Vulnerability

"SQL injection attacks"

sp3x has discovered a vulnerability in PHP-Nuke, which can be exploited by malicious people to conduct SQL injection attacks.

Input passed to the "username" parameter (Nickname field) in the new user registration functionality of the "Your_Account" module isn't properly sanitised before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.

The vulnerability has been confirmed in version 7.8. Other versions may also be affected.

References:
http://securityreason.com/securityalert/440

GNU Tar PAX Extended Headers Handling Buffer Overflow

"Denial of Service"

A vulnerability has been reported in GNU Tar, which potentially can be exploited by malicious people to cause a DoS (Denial of Service) and to compromise a user's system.

The vulnerability is caused due to a boundary error within the handling of PAX extended headers. This can be exploited to cause a buffer overflow.

The vulnerability has been reported in version 1.15.1. Prior versions may also be affected.

References:
http://lists.gnu.org/archive/html/bug-tar/2006-02/msg00051.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.

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