ScoutNews Team **July 15, 2005**
Issue # 28

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

A good 5-step security program, citizen arrested for using neighbor's wi-fi network and DHS gets wise to cyber-security.

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

- **Good advice for network security**

Marcus Shields of Soltrus, Inc. outlines 5 steps to network security. Simple and cost-effective measures to guard against cyber theft. Wireless security is a crucial component.
InformationWeek

Full Story :
http://informationweek.com/story/showArticle.jhtml?articleID=165701841

- **Florida man arrested for stealing Wi-Fi signal**

C'mon you at least have thought of it, right? A resident in St. Petersburg, Fl. Spotted the man sitting in an SUV using a laptop outside of his house and called the police. This type

of crime is so new that the police have not started tracking the incidents. I'm sure that this is not the last that we will hear of this type of crime.

networkingpipeline

Related Links:
http://www.networkingpipeline.com/165700409

- **Cyber Security gets elevated post within Dept. of Homeland Security**

The new position of assistant secretary for cyber security and telecommunications should bring greater focus to the importance for protection of the nation's data infrastructure. This shows a positive step the realization by the administration that information assets are at least equally as important as physical assets.

RedHerring via Technology Daily

Related Links:
http://www.redherring.com/Article.aspx?a=12749&hed=High+Praise+for+Cyber+Security&sector=Industries&subsector=SecurityAndDefense

New Vulnerabilities Tested in SecureScout

- **15642 Mozilla Thunderbird XBL Controls Script Execution Vulnerability (Remote File Checking)**

moz_bug_r_a4 has reported a vulnerability in Thunderbird, which can be exploited by malicious people to bypass certain security restrictions.

The problem is that scripts in XBL controls in e-mails can be executed even when JavaScript has been disabled (JavaScript is disabled by default). This does not pose any direct security risks by itself, but may enable exploitation of vulnerabilities requiring JavaScript.

The vulnerability has been fixed in the CVS repository and will be included in the upcoming 1.0.5 release.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/mfsa2005-46.html

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

Other references:

http://secunia.com/advisories/16062/

CVE Reference: CAN-2005-0230

❖ 15643 Mozilla untrusted events generated Vulnerability (Remote File Checking)

A vulnerability has been reported in Mozilla Suite, 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 where untrusted events generated by web content are delivered to the browser user interface has various impacts.

The vulnerabilities have been fixed in the CVS repository and will be included in the upcoming 1.7.9 release.

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

References:

Original advisory:
http://www.mozilla.org/security/announce/mfsa2005-45.html

Other references:
http://secunia.com/advisories/16059/
http://secunia.com/advisories/14938/

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

CVE Reference: None

❖ 15644 Mozilla Scripts in XBL controls Vulnerability (Remote File Checking)

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

Scripts in XBL controls can be executed even when JavaScript has been disabled.

The vulnerabilities have been fixed in the CVS repository and will be included in the upcoming 1.7.9 release.

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

References:

Original advisory:
http://www.mozilla.org/security/announce/mfsa2005-46.html

Other references:
http://secunia.com/advisories/16059/

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

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

CVE Reference: None

❖ 15645 Mozilla "InstallTrigger.install()" Vulnerability (Remote File Checking)

A vulnerability has been reported in Mozilla Suite, 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, where the callback function of the "InstallTrigger.install()" function is not properly cleared before navigating to a new site, can be exploited to execute arbitrary script code in a user's browser session in context of an arbitrary site.

The vulnerabilities have been fixed in the CVS repository and will be included in the upcoming 1.7.9 release.

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

References:

Original advisory:
http://www.mozilla.org/security/announce/mfsa2005-48.html

Other references:
http://secunia.com/advisories/16059/
http://secunia.com/advisories/14938/

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

CVE Reference: None

❖ 15646 Mozilla "InstallVersion.compareTo()" Vulnerability (Remote File Checking)

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

An input validation error in the handling of unexpected JavaScript objects passed to the "InstallVersion.compareTo()" function may be exploited to execute arbitrary code.

The vulnerabilities have been fixed in the CVS repository and will be included in the upcoming 1.7.9 release.

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

References:

Original advisory:
http://www.mozilla.org/security/announce/mfsa2005-50.html

Other references:
http://secunia.com/advisories/16059/
http://secunia.com/advisories/14938/

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

CVE Reference: None

❖ 15647 Mozilla DOM node names Vulnerability (Remote File Checking)

A vulnerability has been reported in Mozilla Suite, 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.

The vulnerabilities have been fixed in the CVS repository and will be included in the upcoming 1.7.9 release.

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/16059/
http://secunia.com/advisories/14938/

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

CVE Reference: XXXXXXXX

❖ 15648 Mozilla insecure cloning of base objects Vulnerability (Remote File Checking)

A vulnerability has been reported in Mozilla Suite, 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.

The vulnerabilities have been fixed in the CVS repository and will be included in the upcoming 1.7.9 release.

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/16059/
http://secunia.com/advisories/14938/

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

CVE Reference: None

❖ **15649 Firefox untrusted events generated 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 where un-trusted events generated by web content are delivered to the browser user interface has various impacts.

Version 1.0.5 fixes the issue.

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

References:

Original advisory:
http://www.mozilla.org/security/announce/mfsa2005-45.html

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

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

CVE Reference: None

❖ **15650 Firefox XBL controls 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.

Scripts in XBL controls can be executed even when JavaScript has been disabled.

Version 1.0.5 fixes the issue.

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

References:

Original advisory:
http://www.mozilla.org/security/announce/mfsa2005-46.html

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

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

CVE Reference: None

❖ **15651 Firefox "Set As Wallpaper" 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.

The image URL is not properly verified before being used with the "Set As Wallpaper" option. This can be exploited to execute arbitrary script code by tricking a user into setting an image with a specially crafted "javascript:" URL as the wallpaper.

This vulnerability only affects versions 1.0.3 and 1.0.4.

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

References:

Original advisory:
http://www.mozilla.org/security/announce/mfsa2005-47.html

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

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

CVE Reference: None

New Vulnerabilities found this Week

❖ **Microsoft Windows Color Management Module Buffer Overflow**
"Buffer overflow"

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

The vulnerability is caused due to a boundary error within the color management module when validating ICC profile format tags. This can be exploited to cause a buffer overflow by e.g. tricking a user into visiting a malicious web site or view a malicious e-mail message containing a specially crafted image file.

Successful exploitation allows execution of arbitrary code.

NOTE: According to Microsoft, the vulnerability is already being exploited.

References:
http://www.microsoft.com/technet/security/Bulletin/MS05-036.mspx

❖ **Microsoft Word Font Parsing Buffer Overflow Vulnerability**
"Stack-based buffer overflow"

Lord Yup has reported a vulnerability in Microsoft Word, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error within the parsing of fonts. This can be exploited to cause a stack-based buffer overflow by tricking a user into opening a specially crafted Word document.

Successful exploitation allows execution of arbitrary code.

References:
http://www.microsoft.com/technet/security/Bulletin/MS05-035.mspx

❖ **Avaya telnet Two Vulnerabilities**
"Compromise a user's system"

Avaya has acknowledged two vulnerabilities in Intuity Audix, which can be exploited by malicious people to.

References:
http://support.avaya.com/elmodocs2/security/ASA-2005-156.pdf

❖ **Winamp ID3v2 Tag Handling Buffer Overflow Vulnerability**
"Buffer overflow"

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.

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

- **SquirrelMail Insecure Parameters Extraction Vulnerability**
  "Cross-site scripting attacks, and disclose and manipulate sensitive information"

James Bercegay has reported a vulnerability in SquirrelMail, which can be exploited by malicious people to conduct cross-site scripting attacks, and disclose and manipulate sensitive information.

The vulnerability is caused due to an error where parameters are insecurely extracted in options_identities.php. This can be exploited to disclose and manipulate other users' preferences, write files to arbitrary locations, and execute arbitrary HTML and script code in a user's browser session in context of an affected site.

The vulnerability has been reported in versions 1.4.0 through 1.4.5-RC1.

References:
http://www.squirrelmail.org/security/issue/2005-07-13

- **Mozilla Thunderbird XBL Controls Script Execution Vulnerability**
  "Bypass certain security restrictions"

moz_bug_r_a4 has reported a vulnerability in Thunderbird, which can be exploited by malicious people to.

The problem is that scripts in XBL controls in e-mails can be executed even when JavaScript has been disabled (JavaScript is disabled by default). This does not pose any direct security risks by itself, but may enable exploitation of vulnerabilities requiring JavaScript.

References:
http://www.mozilla.org/security/announce/mfsa2005-46.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.
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