netVigilance

ScoutNews Team

October 7, 2005
Issue # 40

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Snort and nessus to enter the commercial market, new holes in AV software, corporate IM users big targets and latest Websense security report is out.

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

- **Sourcefire (Snort) sells for $225M, nessus source to be closed**

Two prominent landmarks of the open-source security software arena announce plans to go commercial. Checkpoint announced that they intend to acquire Sourcefire, the makers of the popular freeware tool Snort.

Sourcefire founder and CTO, Martin Roesch assured the user community that for some time at least; Snort will remain under GPL.: "I'll start by stating again what I've stated in the past, Snort is now and will continue to be free to end-users. We will continue to develop and distribute the Snort engine under the GPL, improve and document the program to stay on the cutting edge and expand the snort.org web site."

Tenable Network Security's' Renaud Deraison; the writer of the nessus freeware vulnerability scanner, announced this week plans to commercialize the next version of the tool and remove it from the GPL licensing model. Citing increased competition from commercial tools causing the development to fall behind Mr. Deraison was quoted saying :"Virtually nobody has ever contributed anything to improve the scanning engine over the last six years,"

Despite the implied protection of the GPL licensing, Tenable is shouldering the development burden for nessus while countless integrators make money off of reselling the tool.

We welcome you to the free western world – *Ed.*
ZDNet

Related Links:
Nessus:
http://news.zdnet.com/2100-3513_22-5890093.html
http://archives.neohapsis.com/archives/nmap/2005/0016.html

Sourcefire:
http://www.crn.com/sections/security/security.jhtml?articleId=171203998
http://www.snort.org/about_snort/msg_from_marty/mr_100605.html

- ### Symantec, Kaspersky disclose open vulnerabilities

In as many days; two Anti Virus vendors disclose vulnerabilities in their products. The Symantec bug could "…allow remote attackers to gain privileged remote access to computers." The Kapersky flaw could enable a hacker to gain complete control of a windows machine protected by the company's products.
TechWeb News

Related Links:

http://www.securitypipeline.com/desktop/171203303

http://www.techweb.com/wire/security/171202971

- ### IM threats grow with corporate adoption

IMlogic Threat Center, a consortium that provides threat detection and protection for IM and peer-to-peer (P2P) apps, reports a whopping 3,295 % increase in attacks against corporate IM users. The Q305 results were compared results from the same period last year.
ADTMag.com

Full Story:
http://www.adtmag.com/article.asp?id=11884

❖ Websense security report out

In it's semi-annual document entitled "Security Trends Report", Websense (San Diego, Calif) claims that Phishing is hot and targeting smaller financial institutions, banks and credit unions.

This trend may be the funnel effect created by improved security at larger organizations.
Internet Week

Related Links:
http://www.internetweek.com/news/171203370

New Vulnerabilities Tested in SecureScout

❖ 13287 CVS zlib "inflate()" and "inflateBack()" Vulnerabilities

CVS is the Concurrent Versions System, the dominant open-source network-transparent version control system.

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

The vulnerability is caused due to the use of a vulnerable version of zlib.

The vulnerability has been reported in version 1.12.12. Prior versions may also be affected.

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

References:

Original advisory:
http://www.nongnu.org/cvs/#TOCdownloading

Other references:
http://secunia.com/advisories/17054/
http://secunia.com/advisories/11129/
http://www.kb.cert.org/vuls/id/238678

Product HomePage:
http://www.nongnu.org/cvs/

CVE Reference: CAN-2004-0797

❖ 13288 CVS zlib "inftrees.c" Vulnerabilities

CVS is the Concurrent Versions System, the dominant open-source network-transparent version control system.

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

The vulnerability is caused due to the use of a vulnerable version of zlib.

The vulnerability has been reported in version 1.12.12. Prior versions may also be affected.

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

References:

Original advisory:
http://www.nongnu.org/cvs/#TOCdownloading

Other references:
http://secunia.com/advisories/17054/
http://secunia.com/advisories/15949/
http://www.gentoo.org/security/en/glsa/glsa-200507-05.xml

Product HomePage:
http://www.nongnu.org/cvs/

CVE Reference: CAN-2005-2096

❖ 15690 Mozilla Firefox Iframe Size Denial of Service Weakness (Remote File Checking)

Tom Ferris has discovered a weakness in Firefox, which can be exploited by malicious people to cause a DoS (Denial of Service).

The weakness is caused due to an error in the handling of overly large size attributes in the "Iframe" tag. This can be exploited to crash a vulnerable browser via a specially crafted "Iframe" tag on a malicious web site.

The weakness has been confirmed in version 1.0.7 on Fedora Core 4 (Linux). Other versions and platforms may also be affected.

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

References:

Original Advisories:
http://security-protocols.com/modules.php?name=News&file=article&sid=2978

Other references:
http://secunia.com/advisories/17071/

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

CVE Reference: None

❖ 15691 Mozilla Firefox processing of XBM images Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox, which can be exploited by malicious people to allows execution of arbitrary code.

A boundary error in the processing of XBM images can be exploited to cause a heap based buffer overflow via a specially crafted image.

The vulnerability has been reported in version 1.0.6. Prior versions may also be affected.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/mfsa2005-58.html

Other references:
http://secunia.com/advisories/16911/
# CONFIRM:http://www.mozilla.org/security/announce/mfsa2005-58.html

# MANDRIVA:MDKSA-2005:169
# URL:http://www.mandriva.com/security/advisories?name=MDKSA-2005:169

# MANDRIVA:MDKSA-2005:170
# URL:http://www.mandriva.com/security/advisories?name=MDKSA-2005:170

# REDHAT:RHSA-2005:785
# URL:http://www.redhat.com/support/errata/RHSA-2005-785.html

# FRSIRT:ADV-2005-1824
# URL:http://www.frsirt.com/english/advisories/2005/1824

# SECTRACK:1014954
# URL:http://securitytracker.com/id?1014954

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

CVE Reference: CAN-2005-270

❖ 15692 Mozilla Firefox processing of Unicode sequences with "zero-

width non-joiner" characters Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox, which can be exploited by malicious people to allows execution of arbitrary code.

An error in the processing of Unicode sequences with "zero-width non-joiner" characters can be exploited to corrupt the stack and cause a crash.

The vulnerability has been reported in version 1.0.6. Prior versions may also be affected.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/mfsa2005-58.html

Other references:
http://secunia.com/advisories/16911/
# CONFIRM:http://www.mozilla.org/security/announce/mfsa2005-58.html

# MANDRIVA:MDKSA-2005:169
# URL:http://www.mandriva.com/security/advisories?name=MDKSA-2005:169

# MANDRIVA:MDKSA-2005:170
# URL:http://www.mandriva.com/security/advisories?name=MDKSA-2005:170

# REDHAT:RHSA-2005:785
# URL:http://www.redhat.com/support/errata/RHSA-2005-785.html

# FRSIRT:ADV-2005-1824
# URL:http://www.frsirt.com/english/advisories/2005/1824

# SECTRACK:1014954
# URL:http://securitytracker.com/id?1014954

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

CVE Reference: CAN-2005-2702

❖ 15693 Mozilla Firefox processing of headers passed to the "XMLHttpRequest" object Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox, which can be exploited by malicious people to Inject arbitrary HTTP requests.

An input validation error in the processing of headers passed to the "XMLHttpRequest" object can be exploited to inject arbitrary HTTP requests.

The vulnerability has been reported in version 1.0.6. Prior versions may also be affected.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/mfsa2005-58.html

Other references:
http://secunia.com/advisories/16911/
# CONFIRM:http://www.mozilla.org/security/announce/mfsa2005-58.html

# MANDRIVA:MDKSA-2005:169
# URL:http://www.mandriva.com/security/advisories?name=MDKSA-2005:169

# MANDRIVA:MDKSA-2005:170
# URL:http://www.mandriva.com/security/advisories?name=MDKSA-2005:170

# REDHAT:RHSA-2005:785
# URL:http://www.redhat.com/support/errata/RHSA-2005-785.html

# FRSIRT:ADV-2005-1824
# URL:http://www.frsirt.com/english/advisories/2005/1824

# SECTRACK:1014954
# URL:http://securitytracker.com/id?1014954

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

CVE Reference: CAN-2005-2703

❖ 15694 Mozilla Firefox XBL control can spoof DOM objects Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox, which can be exploited by malicious people to Spoof DOM objects.

An unspecified error where a XBL control which implements an internal interface can spoof DOM objects.

The vulnerability has been reported in version 1.0.6. Prior versions may also be affected.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/mfsa2005-58.html

Other references:

http://secunia.com/advisories/16911/

# CONFIRM:http://www.mozilla.org/security/announce/mfsa2005-58.html

# MANDRIVA:MDKSA-2005:169
# URL:http://www.mandriva.com/security/advisories?name=MDKSA-2005:169

# MANDRIVA:MDKSA-2005:170
# URL:http://www.mandriva.com/security/advisories?name=MDKSA-2005:170

# REDHAT:RHSA-2005:785
# URL:http://www.redhat.com/support/errata/RHSA-2005-785.html

# FRSIRT:ADV-2005-1824
# URL:http://www.frsirt.com/english/advisories/2005/1824

# SECTRACK:1014954
# URL:http://securitytracker.com/id?1014954

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

CVE Reference: CAN-2005-2704

❖ 15695 Mozilla Firefox integer overflow error in the JavaScript engine Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox, which can be exploited by malicious people to allows execution of arbitrary code.

An unspecified integer overflow error in the JavaScript engine can be exploited to execute arbitrary code.

The vulnerability has been reported in version 1.0.6. Prior versions may also be affected

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/mfsa2005-58.html

Other references:
http://secunia.com/advisories/16911/

# CONFIRM:http://www.mozilla.org/security/announce/mfsa2005-58.html

# MANDRIVA:MDKSA-2005:169
# URL:http://www.mandriva.com/security/advisories?name=MDKSA-2005:169

# MANDRIVA:MDKSA-2005:170
# URL:http://www.mandriva.com/security/advisories?name=MDKSA-2005:170

# REDHAT:RHSA-2005:785
# URL:http://www.redhat.com/support/errata/RHSA-2005-785.html

# FRSIRT:ADV-2005-1824
# URL:http://www.frsirt.com/english/advisories/2005/1824

# SECTRACK:1014954
# URL:http://securitytracker.com/id?1014954

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

CVE Reference: CAN-2005-2705

❖ 15696 Mozilla Firefox unprivileged "about:" pages can load privileged "chrome:" Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox, which can be exploited by malicious people to allows execution of arbitrary code.

The problem is that unprivileged "about:" pages can load privileged "chrome:" pages in certain situations.

This does not pose any security risk by it self, but can be exploited in combination with other cross-site scripting vulnerabilities to execute arbitrary code.

The vulnerability has been reported in version 1.0.6. Prior versions may also be affected

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/mfsa2005-58.html

Other references:
http://secunia.com/advisories/16911/

# CONFIRM:http://www.mozilla.org/security/announce/mfsa2005-58.html

# MANDRIVA:MDKSA-2005:169
# URL:http://www.mandriva.com/security/advisories?name=MDKSA-2005:169

# MANDRIVA:MDKSA-2005:170
# URL:http://www.mandriva.com/security/advisories?name=MDKSA-2005:170

# REDHAT:RHSA-2005:785
# URL:http://www.redhat.com/support/errata/RHSA-2005-785.html

# FRSIRT:ADV-2005-1824
# URL:http://www.frsirt.com/english/advisories/2005/1824

# SECTRACK:1014954

# URL:http://securitytracker.com/id?1014954

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

CVE Reference: CAN-2005-2706

❖ 15697 Mozilla Firefox error in the creation of windows Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox, which can be exploited by malicious people to allows execution of arbitrary code.

An error in the creation of windows can be exploited to open a new window without the address bar and status bar via a reference to a closed window.

Successful exploitation allows bypass of certain security mechanisms designed to protect against phishing attacks.

The vulnerability has been reported in version 1.0.6. Prior versions may also be affected.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/mfsa2005-58.html

Other references:
http://secunia.com/advisories/16911/

# CONFIRM:http://www.mozilla.org/security/announce/mfsa2005-59.html

# MANDRIVA:MDKSA-2005:169
# URL:http://www.mandriva.com/security/advisories?name=MDKSA-2005:169

# MANDRIVA:MDKSA-2005:170
# URL:http://www.mandriva.com/security/advisories?name=MDKSA-2005:170

# REDHAT:RHSA-2005:785
# URL:http://www.redhat.com/support/errata/RHSA-2005-785.html

# FRSIRT:ADV-2005-1824
# URL:http://www.frsirt.com/english/advisories/2005/1824

# SECTRACK:1014954
# URL:http://securitytracker.com/id?1014954

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

CVE Reference: CAN-2005-2707

New Vulnerabilities found this Week

- **Mozilla Firefox Iframe Size Denial of Service Weakness**
  "Denial of Service"

  Tom Ferris has discovered a weakness in Firefox, which can be exploited by malicious people to cause a DoS (Denial of Service).

  The weakness is caused due to an error in the handling of overly large size attributes in the "Iframe" tag. This can be exploited to crash a vulnerable browser via a specially crafted "Iframe" tag on a malicious web site.

  The weakness has been confirmed in version 1.0.7 on Fedora Core 4 (Linux). Other versions and platforms may also be affected.

  References:
  http://security-protocols.com/modules.php?name=News&file=article&sid=2978

- **Microsoft Windows XP Wireless Zero Configuration Wireless Profile Disclosure**
  "Access to certain sensitive information"

  Laszlo Toth has discovered a security issue in Windows XP, which can be exploited by malicious, local users to gain access to certain sensitive information.

  The security issue is caused due to the Wireless Zero Configuration service allowing a non-privileged user to retrieve the configured wireless profiles using the "WZCQueryInterface()" API. The retrieved profile includes the configured SSIDs and WEP keys, or the PMK (Pairwise Master Key) that is used for pre-shared key authentication in WPA (Wi-Fi Protected Access).

  The security issue has been confirmed in Windows XP SP2 with KB893357 installed.

  References:
  http://www.soonerorlater.hu/index.khtml?article_id=62
  http://support.microsoft.com/kb/893357

- **Avaya Products cpio Insecure File Creation Vulnerability**
  "Disclose and manipulate information"

  Avaya has acknowledged a vulnerability in cpio included in some products, which can be exploited by malicious, local users to disclose and manipulate information.

References:
http://support.avaya.com/elmodocs2/security/ASA-2005-212.pdf
http://secunia.com/advisories/14357/

- **UW-imapd Mailbox Name Parsing Buffer Overflow Vulnerability**
  "Denial of Service"

  infamous41md has reported a vulnerability in UW-imapd, which can be exploited by malicious users to cause a DoS (Denial of Service) or compromise a vulnerable system.

  The vulnerability is caused due to a boundary error in the "mail_valid_net_parse_work()" function when copying the user supplied mailbox name to a stack buffer. This can be exploited to cause a stack-based buffer overflow via a specially crafted mailbox name that contains an single opening double-quote character, without the corresponding closing double-quote.

  Successful exploitation allows arbitrary code execution, but requires valid credentials on the IMAP server.

  The vulnerability has been reported in version imap-2004c1. Prior versions may also be affected.

  References:
  www.idefense.com/application/poi/display?id=313&type=vulnerabilities

- **Apache mod_auth_shadow Module "require group" Incorrect Authentication**
  "Bypass certain security restrictions"

  David Herselman has reported a security issue in the mod_auth_shadow module for Apache, which potentially can be exploited by malicious people to bypass certain security restrictions.

  The problem is that the mod_auth_shadow authentication scheme is automatically used when using the "require group" directive in a ".htaccess" file, which may be different than the intended HTTP authentication scheme..

  References:
  http://www.debian.org/security/2005/dsa-844

- **Squid NTLM Authentication Handling Denial of Service**

"Denial of Service"

Mike Diggins has reported a vulnerability in Squid, which potentially can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in handling changes in the authentication scheme when NTLM authentication is used. This may be exploited to crash the service.

References:
http://www.squid-cache.org/bugs/show_bug.cgi?id=1391

- **Linux Kernel URB Handling Denial of Service Vulnerability**
  "Denial of Service"

  A vulnerability and a security issue have been reported in the Linux Kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

  1) An error in handling asynchronous USB access via usbdevio can be exploited to crash the kernel via a process that issues an URB (USB Request Block) from userspace and terminates before the URB returns.

  Successful exploitation requires that the user has permissions to access an USB device.

  2) An error in jiffies comparison in the "ipt_recent.c" netfilter module, when its value is greater than LONG_MAX, may cause ipt_recent netfilter rules to block too early.

  References:
  http://marc.theaimsgroup.com/?l=linux-kernel&m=112766129313883
  http://blog.blackdown.de/2005/05/09/fixing-the-ipt_recent-netfilter-module/

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