netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 23

June 9, 2006

Table of Contents

Product Focus

Apache Chunked Vulnerability Scanner – The Apache Chunked Vulnerability Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the Apache Chunked Encoding buffer overflow.

This Week in Review

Be careful of USB that you find in your parking lot, Stealing Long distance calls moves to VOIP, Uni's Haven for Hackers.

Enjoy reading & 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

- **Social Engineering, the USB Way**

Steve Stasiukonis tells : We recently got hired by a credit union to assess the security of its network. The client asked that we really push hard on the social engineering button. In the past, they'd had problems with employees sharing passwords and giving up information easily. Leveraging our effort in the report was a way to drive the message home to the employees.

The client also indicated that USB drives were a concern, since they were an easy way for employees to steal information, as well as bring in potential vulnerabilities such as viruses and Trojans. Several other clients have raised the same concern, yet few have done much to protect themselves from a rogue USB drive plugging into their network. I wanted to see if we could tempt someone into plugging one into their employer's network.

Dark Reading

Full Story :
http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1

❖ Phone hacker arrested in Miami

NEW YORK The federal authorities arrested a Miami resident Wednesday in what they said was a hacking scheme involving the resale of Internet telephone service.

The suspect, working with at least one other person, was said to have illegally tapped into the lines of legitimate Internet phone companies, saddling them with the expense of extra traffic, while he collected more than $1 million in connection fees.

The case, one of the first involving Internet phone hacking, illustrates how Internet-based communications may be criminally exploited, and raises fresh questions about the security of phone traffic moving over largely unregulated networks.

Prosecutors said that starting in November 2004, Edwin Andres Pena, 23, a Venezuelan who has permanent residency in the United States and lives in Miami, used two companies that he started to offer wholesale phone connections at discounted rates to small Internet phone companies.

Instead of buying access to other networks to connect his clients' calls, Pena is said to have worked with other hackers to create "what amounted to 'free' routes by surreptitiously hacking into the computer networks" of unwitting Internet phone providers, and then routing his customers' calls over those providers' systems, the federal complaint says.

Internation Herald Tribune

Full Story :

http://www.iht.com/articles/2006/06/07/business/voice.php

❖ 21st century university campuses: a haven for hackers and data thieves?

Back when I was at university, when dinosaurs ruled the earth, computer security on the campus was not a concern for most of the students. Apart from having to remember your user name and password for the lab network in Comp. Sci class, there really wasn't much to worry about.

These days, with wireless Internet access, students toting laptops to class, and web-based forms for everything, security has become a major issue on campus. According to

statistics compiled in the United States based on media reports, there have been 29 major security failures on college campuses since January, which compromised information from as many as 845,000 students and staff. This represented 30 percent of all reported security breaches according to ChoicePoint, a data collection firm based out of Georgia. Ironically, ChoicePoint itself has been the victim of data theft in the past.
ZDNet UK

Full Story :

http://arstechnica.com/news.ars/post/20060607-7012.html

New Vulnerabilities Tested in SecureScout

❖ 14718 Mozilla Firefox "Object.watch()" method error, arbitrary JavaScript code execution Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

An error where the "Object.watch()" method exposes the internal "clone parent" function object can be exploited to execute arbitrary JavaScript code with escalated privileges.

The vulnerability has been reported in version 1.0 and 1.5.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2006/mfsa2006-15.html
Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2006-1734

❖ 14719 Mozilla Firefox compilation scope of privileged built-in XBL bindings, arbitrary JavaScript code execution Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

An error in the protection of the compilation scope of built-in privileged XBL bindings can be exploited to execute arbitrary JavaScript code with escalated privileges.

The vulnerability has been reported in version 1.0 and 1.5.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2006/mfsa2006-16.html

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

CVE Reference: CVE-2006-1733

❖ 14720 Mozilla Firefox window.controllers array, arbitrary HTML and script code execution Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

An unspecified error can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an arbitrary site via the window.controllers array.

The vulnerability has been reported in version 1.0 and 1.5.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2006/mfsa2006-17.html

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

CVE Reference: CVE-2006-1732

❖ 14721 Mozilla Firefox "nsHTMLContentSink.cpp", memory corruption Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

An error in the processing of a certain sequence of HTML tags in "nsHTMLContentSink.cpp" can be exploited to cause a memory corruption.

Successful exploitation allows execution of arbitrary code.

The vulnerability has been reported in version 1.0 and 1.5.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2006/mfsa2006-18.html

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

CVE Reference: CVE-2006-0749

❖ 14722 Mozilla Firefox "valueOf.call()" and "valueOf.apply()" methods, arbitrary HTML and script code execution Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

An error in the "valueOf.call()" and "valueOf.apply()" methods can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an arbitrary site.

The vulnerability has been reported in version 1.0 and 1.5.

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

References:

Original advisory:
http://www.mozilla.org/security/announce/2006/mfsa2006-19.html

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

CVE Reference: CVE-2006-1731

❖ 14723 Mozilla Firefox errors in the DHTML implementation, memory corruption Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

Some errors in the DHTML implementation can be exploited to cause a memory corruption.

Successful exploitation may allow execution of arbitrary code.

The vulnerability has been reported in version 1.0 and 1.5.

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

References:

Original advisory:
http://www.mozilla.org/security/announce/2006/mfsa2006-20.html

Other references:
* DEBIAN:DSA-1046
* URL:http://www.debian.org/security/2006/dsa-1046
* DEBIAN:DSA-1051
* URL:http://www.debian.org/security/2006/dsa-1051
* CERT-VN:VU#350262
* URL:http://www.kb.cert.org/vuls/id/350262
* BID:17516

* URL:http://www.securityfocus.com/bid/17516
* FRSIRT:ADV-2006-1356
* URL:http://www.frsirt.com/english/advisories/2006/1356
* SECTRACK:1015919
* URL:http://securitytracker.com/id?1015919
* SECTRACK:1015921
* URL:http://securitytracker.com/id?1015921
* SECTRACK:1015920
* URL:http://securitytracker.com/id?1015920
* SECUNIA:19631
* URL:http://secunia.com/advisories/19631
* SECUNIA:19649
* URL:http://secunia.com/advisories/19649
* SECUNIA:19863
* URL:http://secunia.com/advisories/19863
* SECUNIA:19941
* URL:http://secunia.com/advisories/19941
* MISC: https://bugzilla.mozilla.org/show_bug.cgi?id=326834
* MISC: https://bugzilla.mozilla.org/show_bug.cgi?id=326615
* MISC: https://bugzilla.mozilla.org/show_bug.cgi?id=315254

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

CVE Reference: CVE-2006-1529
CVE-2006-1530
CVE-2006-1531
CVE-2006-1723

❖ 14724 Mozilla Firefox processing of the CSS letter-spacing property, heap-based buffer overflow Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

An integer overflow error in the processing of the CSS letter-spacing property can be exploited to cause a heap-based buffer overflow.

Successful exploitation allows execution of arbitrary code.

The vulnerability has been reported in version 1.0 and 1.5.

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

References:

Original advisory:
http://www.mozilla.org/security/announce/2006/mfsa2006-22.html

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

CVE Reference: CVE-2006-1730

❖ 14725 Mozilla Firefox file upload controls, upload arbitrary files Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

An error in the handling of file upload controls can be exploited to upload arbitrary files from a user's system by e.g. dynamically changing a text input box to a file upload control.

The vulnerability has been reported in version 1.0 and 1.5.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2006/mfsa2006-23.html
http://www.mozilla.org/security/announce/2006/mfsa2006-41.html

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-1729
CVE-2006-2782

❖ 14726 Mozilla Firefox "crypto.generateCRMFRequest()", arbitrary code execution Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

An unspecified error in the "crypto.generateCRMFRequest()" method can be exploited to execute arbitrary code.

The vulnerability has been reported in version 1.0 and 1.5.

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

References:

Original advisory:
http://www.mozilla.org/security/announce/2006/mfsa2006-24.html

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

CVE Reference: CVE-2006-1728

❖ 14727 Mozilla Firefox handling of scripts in XBL controls, privileges escalation Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

An error in the handling of scripts in XBL controls can be exploited to gain chrome privileges via the "Print Preview" functionality.

The vulnerability has been reported in version 1.0 and 1.5.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/2006/mfsa2006-25.html

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

CVE Reference: CVE-2006-1727

New Vulnerabilities found this Week

Courier Mail Server Username Encoding Denial of Service

“Denial of Service”

A vulnerability has been reported in Courier Mail Server, which potentially can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error within the encoding of usernames that contain the "=" character. This can potentially be exploited to cause a DoS by consuming large amount of CPU resources.

The vulnerability has been reported in versions prior to 0.53.2.

References:
http://www.courier-mta.org/beta/patches/verp-fix/README.txt
http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=368834

LibTIFF tiff2pdf Buffer Overflow Vulnerability

“Denial of Service”

gpe92 has discovered a vulnerability in LibTIFF, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a user's system.

The vulnerability is caused due to a boundary error within tiff2pdf when handling a TIFF file with a "DocumentName" tag that contains UTF-8 characters. This can be exploited to cause a stack-based buffer overflow and may allow arbitrary code execution.

The vulnerability has been confirmed in version 3.8.2. Other versions may also be affected.

References:
http://bugzilla.remotesensing.org/show_bug.cgi?id=1196

Microsoft NetMeeting Denial of Service Vulnerability
“Denial of Service”

HexView has reported a vulnerability in Microsoft NetMeeting, which can be exploited by malicious users to cause a DoS (Denial of Service).

The vulnerability is caused due to an error within the handling of certain received data. This can be exploited to overwrite application memory, which causes the application to crash or to consume a large amount of CPU resources.

The vulnerability has been reported in version 3.01. Other versions may also be affected.

References:
http://www.hexview.com/docs/20060606-1.txt

Firefox File Upload Form Keystroke Event Cancel Vulnerability
“disclosing sensitive information”

Charles McAuley has reported a vulnerability in Firefox, which can be exploited by malicious people to trick users into disclosing sensitive information.

The vulnerability is caused due to a design error where a script can cancel certain keystroke events when entering text. This can be exploited to trick a user into typing a filename in a file upload input field by changing focus and cancel the "OnKeyPress" JavaScript event on certain characters.

Successful exploitation allows an arbitrary file on the user's system to be uploaded to a malicious web site, but requires that the user types a text containing the characters of the filename.

The vulnerability has been confirmed in version 1.5.0.4. Other versions may also be affected.

References:
http://lists.grok.org.uk/pipermail/full-disclosure/2006-June/046610.html

SpamAssassin "spamd" Shell Command Injection Vulnerability
“inject arbitrary shell commands”

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

Some unspecified input is not properly sanitized before being used. This can be exploited to inject arbitrary shell commands.

Successful exploitation requires that spamd is used with the "--vpopmail" and "--paranoid" switches.

The vulnerability has been reported in version 3.0.3. Other versions may also be affected.

References:
http://www.nabble.com/ANNOUNCE%3A-Apache-SpamAssassin-3.1.3-available%21-t1736096.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