netVigilance
assurance has arrived

2006 Issue # 21

ScoutNews

The weekly Security update from the makers of SecureScout

May 26, 2006

Table of Contents

Product Focus

Spida Digispid Worm Scanner – The Sasser Worm 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 Microsoft SSL Vulnerablility (MS04-011) that used by the Sasser Worm to infect machines.

This Week in Review

High Risk Vuln in Symantec AV, Anti Piracy MPAA accused of hacking, Teens try to blackmail MySpace over security flaw.

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

- **Company: Hackers can crack top antivirus program**

Symantec Corp.'s leading antivirus software, which protects some of the world's largest corporations and U.S. government agencies, suffers from a flaw that lets hackers seize control of computers to steal sensitive data, delete files or implant malicious programs, researchers said Thursday.

Symantec said it was investigating the issue but could not immediately corroborate the vulnerability. If confirmed, the threat to computer users would be severe because the security software is so widely used and because no action is required by victims using the latest versions of Symantec Antivirus to suffer a crippling attack over the Internet.

Symantec has boasted that its antivirus products are installed on more than 200 million computers. A spokesman, Mike Bradshaw, said the company was examining the reported flaw but described it as "so new that we don't have any details."

CNN technology

Full Story :
http://www.cnn.com/2006/TECH/internet/05/25/antivirus.flaw.ap/index.html

❖ Lawsuit says movie group hired hacker

A popular Web site that helps users search and find links where they can download certain files -- including pirated television shows and films -- is suing the Motion Picture Association of America, accusing the group of paying a hacker to break into the site's computers.

Torrentspy.com, part of Valence Media, said in its lawsuit in U.S. District Court for Central California that the motion picture group hired an unnamed person for $15,000 to steal passwords, e-mails and detailed information about the company's finances and operations.

San Francisco Chronicle

Full Story :

http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/05/26/BUGHIJ282626.DTL

❖ Teens charged over MySpace blackmail

“$150,000 or we tell everyone how to steal personal details”

Two US teenagers have been charged with attempted extortion and illegal computer access following an attempt to blackmail social networking site MySpace.com.

Shaun Harrison, 18, and Saverio Mondelli, 19, both from Suffolk County, New York, are accused of threatening to reveal how to steal personal information from MySpace unless a ransom of $150,000 was paid.

E-Commerce News

Full Story :

http://www.vnunet.com/vnunet/news/2157037/teens-charged-myspace-blackmail

New Vulnerabilities Tested in SecureScout

❖ 16248 QuickTime Code Execution Vulnerability within the processing of BMP images (Remote File Checking)

A vulnerability has been reported in QuickTime, which can be exploited by malicious people to execute arbitrary code.

A boundary error within the processing of BMP images can be exploited via a specially crafted BMP image to crash the application and potentially execute arbitrary code.

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

References:

Original Advisory:
* APPLE:APPLE-SA-2006-05-11
http://lists.apple.com/archives/security-announce/2006/May/msg00002.html

Other references:
* MISC: http://www.security-protocols.com/sp-x27-advisory.php
* BID:17953
* URL:http://www.securityfocus.com/bid/17953
* OSVDB:24820
* URL:http://www.osvdb.org/24820
* SECTRACK:1016067
* URL:http://securitytracker.com/id?1016067
* SECUNIA:20069
* URL:http://secunia.com/advisories/20069

Product:
http://www.apple.com/quicktime/

CVE Reference: CVE-2006-2238

❖ 16249 Mozilla Firefox error in the "QueryInterface" method to cause a memory corruption Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

An error in the "QueryInterface" method of the Location and Navigator objects can be exploited to cause a memory corruption.

Successful exploitation allows execution of arbitrary code.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2006/mfsa2006-04.html

Other references:
* CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=319296
* CERT-VN:VU#759273
* URL:http://www.kb.cert.org/vuls/id/759273
* 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-queryinterface-memory-corruption(24433)
* URL:http://xforce.iss.net/xforce/xfdb/24433

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

CVE Reference: CVE-2006-0295

❖ 16250 Mozilla Firefox arbitrary XML and JavaScript code injection Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

An input validation error in the processing of the attribute name when calling "XULDocument.persist()" can be exploited to inject arbitrary XML and JavaScript code in "localstore.rdf", which will be executed with the permissions of the browser the next time the browser starts up again.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/mfsa2006-05.html

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

CVE Reference: CVE-2006-0296

❖ 16251 Mozilla Firefox E4X, SVG, and Canvas functionalities arbitrary

code execution Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

Some integer overflows in the E4X, SVG, and Canvas functionalities may be exploited to execute arbitrary code.

The vulnerability has been reported in version 1.5

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/mfsa2006-06.html

Other references:
* CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=319872
* CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=322215
* 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-component-integer-overflow(24435)
* URL:http://xforce.iss.net/xforce/xfdb/24435

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

CVE Reference: CVE-2006-0297

❖ 16252 Mozilla Firefox XML parser information disclosure Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

A boundary error in the "nsExpatDriver::ParseBuffer()" function in the XML parser may be exploited to disclose data on the heap.

The vulnerability has been reported in version 1.5.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/mfsa2006-07.html

Other references:
* 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-xml-parser-dos(24436)
* URL:http://xforce.iss.net/xforce/xfdb/24436

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

CVE Reference: CVE-2006-0298

❖ 16253 Mozilla Firefox Code execution Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

An error exists where JavaScript can be injected into another page, which is currently loading. This 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 Advisories:
http://www.mozilla.org/security/announce/2006/mfsa2006-09.html

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

CVE Reference: CVE-2006-1741

❖ 16254 Mozilla Firefox JavaScript engine garbage collection Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

An error in the garbage collection in the JavaScript engine 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 Advisories:
http://www.mozilla.org/security/announce/2006/mfsa2006-10.html

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

CVE Reference: CVE-2006-1742

❖ 16255 Mozilla Firefox CSS border rendering implementation boundary error Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

A boundary error in the CSS border rendering implementation may be exploited to write past the end of an 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 Advisory:
http://www.mozilla.org/security/announce/2006/mfsa2006-11.html

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

CVE Reference: CVE-2006-1739

❖ 16256 Mozilla Firefox handling of regular expressions Code execution Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

An integer overflow in the handling of overly long regular expressions in JavaScript may be exploited to execute arbitrary JavaScript bytecode.

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/mfsa2006-11.html

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

CVE Reference: CVE-2006-1737

❖ 16257 Mozilla Firefox handling of display styles arbitrary code execution Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

Two errors in the handling of "-moz-grid" and "-moz-grid-group" display styles may 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 Advisories:
http://www.mozilla.org/security/announce/2006/mfsa2006-11.html

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

CVE Reference: CVE-2006-1738

New Vulnerabilities found this Week

Microsoft Word Malformed Object Code Execution Vulnerability

"Execute arbitrary code"

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

The vulnerability is caused due to an unspecified error when handling malformed objects in a specially crafted Word document. This can be exploited to execute arbitrary code.

NOTE: This vulnerability is being actively exploited.

The vulnerability has been reported in Microsoft Word 2002 and Microsoft Word 2003.

References:
http://www.microsoft.com/technet/security/advisory/919637.mspx
http://isc.sans.org/diary.php?storyid=1345
http://www.kb.cert.org/vuls/id/446012

Cisco VPN Client Privilege Escalation Vulnerability
“Gain escalated privileges”

A vulnerability has been reported in Cisco VPN Client, which can be exploited by malicious, local users to gain escalated privileges on a vulnerable system.

The vulnerability is caused due to an unspecified error in the GUI (also known as the "VPN client dialer") and can be exploited to execute arbitrary commands with SYSTEM privileges.

The vulnerability has been reported in versions 2.x, 3.x, 4.0.x, 4.6.x, 4.7.x (except version 4.7.00.0533), and 4.8.00.x for Windows.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20060524-vpnclient.shtml

mpg123 "III_i_stereo()" Function Buffer Overflow Vulnerability
“Execution of arbitrary code”

A. Alejandro Hernández has reported a vulnerability in mpg123, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error within the "III_i_stereo()" function in layer3.c when processing MPEG 2.0 layer 3 files. This can be exploited to cause a buffer overflow when a user opens a specially crafted MPEG 2.0 layer 3 file.

Successful exploitation may allow execution of arbitrary code.

References:
http://secunia.com/advisories/20240/

Linux Kernel SNMP NAT Helper Denial of Service
“Denial of Service”

A vulnerability has been reported in the Linux Kernel, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to some errors within the "snmp_trap_decode()" function when handling certain SNMP packets. This can be exploited to cause memory corruption due to incorrect freeing of memory, which can potentially cause the system to crash.

Successful exploitation requires that the "ip_nat_snmp_basic" module is loaded and that traffic NAT is enabled on port 161 or 162.

References:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.18
http://www.kernel.org/git/?p=linux/kernel/git/stable/linux-2.6.16.y.git;a=commit;h=1db6b5a66e93ff125ab871d6b3f7363412cc87e8

Linux Kernel Netfilter Weakness and Two SCTP Vulnerabilities
“Denial of Service; disclose potentially sensitive information”

Two vulnerabilities and a weakness have been reported in the Linux Kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service) and disclose potentially sensitive information, and by malicious people to cause a DoS.

1) An input validation error in SCTP when processing a HB-ACK chunk with a specially-crafted parameter length can be exploited to cause out-of-bounds

memory access. This can potentially cause the system to crash.

2) An error in SCTP chunk length calculation during parameter processing can be exploited to cause out-of-bounds memory access. This can potentially cause the system to crash.

3) A race condition in the "do_add_counters()" function in netfilter can be exploited by local users to read kernel memory or cause the system to crash via a race condition that produces a size value that is different from the size of the allocated memory.

Successful exploitation requires that the user is granted CAP_NET_ADMIN rights.

References:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.17

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