netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 37

September 15, 2006

Table of Contents

Product Focus

- **Delta reporting released in SecureScout SP**

From our release notes:
We have added two new pages to the HTML version of
the Test Job Report: New Vulnerabilities, and Missing Vulnerabilities.
These pages are most useful when used on successive reports, to track changes noted between individual reports.

ASN.1 Vulnerability Scanner – The ASN.1 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 MS04-007 that could allow remote code execution.

This Week in Review

PCI vendors at work. EU commission worries. Spammers change domains faster than... Hackers and other types of criminals team up.

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

❖ Changes Will Improve PCI Security, But Not Enough

A new security organization and an updated standard mark a step forward for the Payment Card Industry initiative. But the entire PCI process needs improvements, especially in communications with stakeholders.

On 7 September 2006, American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International announced the creation of the Payment Card Industry (PCI) Security Standards Council, an independent body that will manage updates to the PCI Data Security Standard and also maintain lists of approved scanning vendors and qualified security assessors (tasks previously handled by MasterCard and Visa, respectively). The newly formed council also announced the release of PCI 1.1, the first update to the PCI Data Security standard.

Gartner Group

Full Story :
http://www.gartner.com/DisplayDocument?doc_cd=143436

❖ Commission concerned about Vista security

Microsoft has fallen foul of the European Commission yet again over plans for its Vista operating system.

The European Commission is concerned that the tech giant's plans to include certain security features in its new operating system goes against competition regulations, mainly that the included security features will lock out competitors from providing alternatives for consumers.
Microsoft has already hit back at the Commission's concerns in a statement that expressed the company's worries that European consumers would miss out on the added security features provided by Vista.

IT Observer

Full Story :
http://www.it-observer.com/news.php?id=6816

❖ Spammers Step Use Of Disposable Domains

According to trend research conducted by security software vendor McAfee, spammers have increased the number of disposable domains that they use and are cycling through new domains faster than in the past. While this trend is certainly a boon for domain name registrars it is in fact a bain for recipients of email as well as mail system administrators.

McAfee said that according to their data major spam campaigns are using 72 percent more domains per hour on average than one month ago. Spammers are apparently trying to outwit URL blacklist filtering systems by stepping up the pace by which such filtering systems must become updated.

"It's a cat and mouse game where spammers try to change their URLs faster than the

anti-spam companies can react," said Guy Roberts, development manager at McAfee, Inc. "If it takes traditional blacklists fifteen to twenty minutes to block a site, then that's how fast the spammers need to change their URLs. Since domains cost only $6 per registration, the spammer is spending less than $100 for four hours of advertising."

WindowsITPro

Full Story :
http://www.windowsitpro.com/Article/ArticleID/93518/93518.html

- **DOJ prosecutor: Criminals teaming up with hackers**

Criminals working with computer hackers pose a rising threat to businesses and governments as those entities increase their dependence on IT systems, a top federal prosecutor says.

"There's always this worry, and I think a legitimate worry, that terrorists will actually launch computer attacks on critical infrastructure," said Christopher Painter, principal deputy chief of the Department of Justice's Computer Crime and Intellectual Property Section.

Painter, who prosecuted famed hacker Kevin Mitnick before he signed a plea agreement, cited a case where a hacker in Australia fouled a fresh water supply in 2000 by hacking into a wireless connection and releasing tons of sewage.

In the U.S. in 1997, a juvenile hacked into a computer phone and data system and turned off the runway lights at an airport in Worcester, Massachusetts, Painter said.

"That obviously could have had pretty dire consequences," Painter said, who spoke about cybercrime at the Information Security Systems Association conference in London.

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9003303&taxonomyId=17&intsrc=kc_feat

New Vulnerabilities Tested in SecureScout

- **12137 Cisco VPN 3000 Concentrator FTP Management Vulnerabilities (CSCse10733/CSCse10753)**

The Cisco VPN 3000 series concentrators are a family of purpose-built, remote access Virtual Private Network (VPN) platforms for data encryption and authentication.

The File Transfer Protocol is an application-layer protocol that allows transfer of files between TCP/IP hosts. It uses Transmission Control Protocol (TCP) as the transport protocol and supports user authentication.

The Cisco VPN 3000 series concentrators can be configured to use the FTP protocol to manage files stored on the concentrator, like configuration files and certificates. Files can be uploaded to, or downloaded from, the concentrator for backup and configuration purposes.

Two vulnerabilities affect the Cisco VPN 3000 series concentrators when FTP is enabled as a file management protocol. By exploiting these vulnerabilities, an attacker could execute the following FTP commands:

* CWD - Change working directory
* MKD - Create (make) a directory
* CDUP - Change directory to the directory one level up
* RNFR - Rename file
* SIZE - Get file size
* RMD - Remove directory

Successful exploitation of these vulnerabilities may allow an attacker to:

* Perform network reconnaissance via the CWD, CDUP, and SIZE FTP commands.
* Change the configuration of the concentrator by renaming or deleting configuration and certificate files via the RNFR and RMD FTP commands.

Please note that since none of these vulnerabilities allows an attacker to upload or download files to/from the concentrator, it is not possible to obtain the configuration of a device or to upload a modified configuration by exploiting the vulnerabilities.

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

References:

References:
* Cisco Security Advisory Cisco VPN 3000 Concentrator Multiple Vulnerabilities (CSCse10733/CSCse10753):
http://www.cisco.com/en/US/products/products_security_advisory09186a0080718330.shtml

CVE Reference:

❖ 16327 Vulnerability in Pragmatic General Multicast (PGM) Could Allow Remote Code Execution (MS06-052/919007) (Remote File Checking)

There is a remote code execution vulnerability that could allow an attacker to send a specially crafted multicast message to an affected system and execute code on the affected system. The MSMQ service, which is the Windows service needed to allow PGM communications is not installed by default.

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

References:

Original advisory:
MS:MS06-052
URL:http://www.microsoft.com/technet/security/Bulletin/MS06-052.mspx

Other references:
CERT:TA06-255A

URL:http://www.us-cert.gov/cas/techalerts/TA06-255A.html
CERT-VN:VU#455516
URL:http://www.kb.cert.org/vuls/id/455516
FRSIRT:ADV-2006-3563
URL:http://www.frsirt.com/english/advisories/2006/3563
SECUNIA:21851
URL:http://secunia.com/advisories/21851

CVE Reference: CVE-2006-3442

❖ 16328 Vulnerability in Indexing Service Could Allow Cross-Site Scripting (MS06-053/920685) (Remote File Checking)

There is an information disclosure vulnerability in the Indexing Service because of the way that it handles query validation. The vulnerability could allow an attacker to run client-side script on behalf of a user. The script could spoof content, disclose information, or take any action that the user could take on the affected Web site.

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

References:

Original advisory:
MS:MS06-053
URL:http://www.microsoft.com/technet/security/Bulletin/MS06-053.mspx

Other references:
CERT:TA06-255A
URL:http://www.us-cert.gov/cas/techalerts/TA06-255A.html
CERT-VN:VU#108884
URL:http://www.kb.cert.org/vuls/id/108884
BID:19927
URL:http://www.securityfocus.com/bid/19927
FRSIRT:ADV-2006-3564
URL:http://www.frsirt.com/english/advisories/2006/3564
SECUNIA:21861
URL:http://secunia.com/advisories/21861

CVE Reference: CVE-2006-0032

❖ 16329 IMail Vulnerability in Microsoft Publisher Could Allow Remote Code Execution (MS06-054/910729) (Remote File Checking)

A remote code execution vulnerability exists in Publisher. An attacker could exploit this vulnerability when Publisher parses a file with a malformed string.

If a user were logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new

accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

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

References:

Original advisory:
MS:MS06-054
URL:http://www.microsoft.com/technet/security/Bulletin/MS06-054.mspx

Other references:
BUGTRAQ:20060912 Computer Terrorism (UK) :: Incident Response Centre - Microsoft Publisher Font Parsing Vulnerability
URL:http://www.securityfocus.com/archive/1/archive/1/445824/100/0/threaded
MISC: http://www.computerterrorism.com/research/ct12-09-2006-2.htm
CERT:TA06-255A
URL:http://www.us-cert.gov/cas/techalerts/TA06-255A.html
CERT-VN:VU#406236
URL:http://www.kb.cert.org/vuls/id/406236
BID:19951
URL:http://www.securityfocus.com/bid/19951
FRSIRT:ADV-2006-3565
URL:http://www.frsirt.com/english/advisories/2006/3565
SECUNIA:21863
URL:http://secunia.com/advisories/21863

CVE Reference: CVE-2006-0001

❖ 16330 QuickTime Code Execution Vulnerability within the processing of H.264 stream (Remote File Checking)

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

Errors in the processing of H.264 movies can be exploited to trigger an integer overflow or buffer overflow.

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

References:

Original Advisory:
APPLE:APPLE-SA-2006-09-12
URL:http://lists.apple.com/archives/Security-announce/2006/Sep/msg00000.html

Other references:
* BUGTRAQ:20060912 Apple QuickTime H.264 Integer Overflow Vulnerability
* URL:http://www.securityfocus.com/archive/1/archive/1/445830/100/0/threaded
* MISC: http://secway.org/advisory/AD20060912.txt
* APPLE:APPLE-SA-2006-09-12

* URL:http://lists.apple.com/archives/Security-announce/2006/Sep/msg00000.html
* BID:19976
* URL:http://www.securityfocus.com/bid/19976
* FRSIRT:ADV-2006-3577
* URL:http://www.frsirt.com/english/advisories/2006/3577
* SECUNIA:21893
* URL:http://secunia.com/advisories/21893
* BUGTRAQ:20060912 Apple QuickTime Player H.264 Codec Remote Integer Overflow
* URL:http://www.securityfocus.com/archive/1/archive/1/445823/100/0/threaded
* BUGTRAQ:20060913 Multiple Vulnerabilities in Apple QuickTime
* URL:http://www.securityfocus.com/archive/1/archive/1/445888/100/0/threaded
* MISC: http://piotrbania.com/all/adv/quicktime-integer-overflow-h264-adv-7.1.txt
* CERT:TA06-256A
* URL:http://www.us-cert.gov/cas/techalerts/TA06-256A.html
* CERT-VN:VU#554252
* URL:http://www.kb.cert.org/vuls/id/554252

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

CVE Reference: CVE-2006-4381

❖ 16331 QuickTime Code Execution Vulnerability within the processing of QuickTime stream (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 QuickTime movies can be exploited to cause a buffer overflow.

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

References:

Original Advisory:
APPLE:APPLE-SA-2006-09-12
URL:http://lists.apple.com/archives/Security-announce/2006/Sep/msg00000.html

Other references:
BUGTRAQ:20060913 Multiple Vulnerabilities in Apple QuickTime
URL:http://www.securityfocus.com/archive/1/archive/1/445888/100/0/threaded
CERT:TA06-256A
URL:http://www.us-cert.gov/cas/techalerts/TA06-256A.html
CERT-VN:VU#683700
URL:http://www.kb.cert.org/vuls/id/683700
BID:19976
URL:http://www.securityfocus.com/bid/19976
FRSIRT:ADV-2006-3577
URL:http://www.frsirt.com/english/advisories/2006/3577
SECUNIA:21893

URL:http://secunia.com/advisories/21893

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

CVE Reference: CVE-2006-4382

❖ 16332 QuickTime Code Execution Vulnerability within the processing of FLC stream (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 FLC movies can be exploited to cause a heap-based buffer overflow via a FLC movie with a specially crafted COLOR_64 chunk.

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

References:

Original Advisory:
APPLE:APPLE-SA-2006-09-12
URL:http://lists.apple.com/archives/Security-announce/2006/Sep/msg00000.html

Other references:
IDEFENSE:20060912 Apple QuickTime FLIC File Heap Overflow Vulnerability
URL:http://www.idefense.com/intelligence/vulnerabilities/display.php?id=413
BUGTRAQ:20060913 Multiple Vulnerabilities in Apple QuickTime
URL:http://www.securityfocus.com/archive/1/archive/1/445888/100/0/threaded
BID:19976
URL:http://www.securityfocus.com/bid/19976
FRSIRT:ADV-2006-3577
URL:http://www.frsirt.com/english/advisories/2006/3577
SECUNIA:21893
URL:http://secunia.com/advisories/21893

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

CVE Reference: CVE-2006-4384

❖ 16333 QuickTime Code Execution Vulnerability within the processing of FlashPix files (Remote File Checking)

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

Errors within the processing of FlashPix files can be exploited to cause an integer overflow or buffer overflow.

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

References:

Original Advisory:
APPLE:APPLE-SA-2006-09-12
URL:http://lists.apple.com/archives/Security-announce/2006/Sep/msg00000.html

Other references:
BUGTRAQ:20060913 Multiple Vulnerabilities in Apple QuickTime
URL:http://www.securityfocus.com/archive/1/archive/1/445888/100/0/threaded
BID:19976
URL:http://www.securityfocus.com/bid/19976
FRSIRT:ADV-2006-3577
URL:http://www.frsirt.com/english/advisories/2006/3577
SECUNIA:21893
URL:http://secunia.com/advisories/21893

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

CVE Reference: CVE-2006-4388

❖ 16334 QuickTime Code Execution Vulnerability within the processing of FlashPix image files (Remote File Checking)

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

An error within the processing of FlashPix files can be exploited to trigger an exception leaving an uninitialised object.

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

References:

Original Advisory:
APPLE:APPLE-SA-2006-09-12
URL:http://lists.apple.com/archives/Security-announce/2006/Sep/msg00000.html

Other references:
BUGTRAQ:20060913 Multiple Vulnerabilities in Apple QuickTime
URL:http://www.securityfocus.com/archive/1/archive/1/445888/100/0/threaded
CERT:TA06-256A
URL:http://www.us-cert.gov/cas/techalerts/TA06-256A.html
CERT-VN:VU#540348
URL:http://www.kb.cert.org/vuls/id/540348
BID:19976
URL:http://www.securityfocus.com/bid/19976
FRSIRT:ADV-2006-3577
URL:http://www.frsirt.com/english/advisories/2006/3577
SECUNIA:21893
URL:http://secunia.com/advisories/21893

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

CVE Reference: CVE-2006-4389

❖ **16335 QuickTime Code Execution Vulnerability within the processing of SGI 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 SGI images can be exploited to cause a buffer overflow.

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

References:

Original Advisory:
APPLE:APPLE-SA-2006-09-12
URL:http://lists.apple.com/archives/Security-announce/2006/Sep/msg00000.html

Other references:
BUGTRAQ:20060913 Multiple Vulnerabilities in Apple QuickTime
URL:http://www.securityfocus.com/archive/1/archive/1/445888/100/0/threaded
APPLE:APPLE-SA-2006-09-12
URL:http://lists.apple.com/archives/Security-announce/2006/Sep/msg00000.html
BID:19976
URL:http://www.securityfocus.com/bid/19976
FRSIRT:ADV-2006-3577
URL:http://www.frsirt.com/english/advisories/2006/3577
SECUNIA:21893
URL:http://secunia.com/advisories/21893

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

CVE Reference: CVE-2006-4385

New Vulnerabilities found this Week

Apple QuickTime Multiple Vulnerabilities

"Code Execution"

Multiple vulnerabilities have been reported in Apple QuickTime, which can be exploited by malicious people to compromise a user's system.

1) Errors in the processing of H.264 movies can be exploited to trigger an integer overflow or buffer overflow.

2) A boundary error within the processing of QuickTime movies can be exploited to

cause a buffer overflow.

3) A boundary error within the processing of FLC movies can be exploited to cause a heap-based buffer overflow via a FLC movie with a specially crafted COLOR_64 chunk.

4) Errors within the processing of FlashPix files can be exploited to cause an integer overflow or buffer overflow.

5) An error within the processing of FlashPix files can be exploited to trigger an exception leaving an uninitialized object.

6) A boundary error within the processing of SGI images can be exploited to cause a buffer overflow.

Successful exploitation of the vulnerabilities may allow execution of arbitrary code.

References:
http://docs.info.apple.com/article.html?artnum=304357
http://www.idefense.com/intelligence/vulnerabilities/display.php?id=413
http://www.reversemode.com/index.php?option=com_remository&Itemid=2&func=fileinfo&id=25
http://pb.specialised.info/all/adv/quicktime-integer-overflow-h264-adv-7.1.txt
http://www.kb.cert.org/vuls/id/540348
http://www.kb.cert.org/vuls/id/554252
http://www.kb.cert.org/vuls/id/683700
http://www.kb.cert.org/vuls/id/200316
http://www.kb.cert.org/vuls/id/308204
http://descriptions.securescout.com/tc/16330
http://descriptions.securescout.com/tc/16331
http://descriptions.securescout.com/tc/16332
http://descriptions.securescout.com/tc/16333
http://descriptions.securescout.com/tc/16334
http://descriptions.securescout.com/tc/16335

Internet Explorer daxctle.ocx "KeyFrame()" Method Vulnerability

“Memory corruption error; execution of arbitrary code”

nop has discovered a vulnerability in Internet Explorer, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a memory corruption error in the Microsoft Multimedia Controls ActiveX control (daxctle.ocx) in the "CPathCtl::KeyFrame()" function. This can be exploited by e.g. tricking a user into viewing a malicious HTML document passing specially crafted arguments to the ActiveX control's "KeyFrame()" method.

Successful exploitation allows execution of arbitrary code.

It is also possible to crash the browser via the "Spline()" method.

References:
http://www.xsec.org/index.php?module=releases&act=view&type=2&id=20

Symantec Products Alert Notification Two Vulnerabilities

“Denial of Service”

Some vulnerabilities have been reported in Symantec Client Security and Symantec AntiVirus Corporate Edition, which can be exploited by malicious, local users to cause a DoS (Denial of Service) or gain escalated privileges.

1) A format string error within the handling of "Tamper Protection" and "Virus Alert Notification" messages can be exploited to execute arbitrary code with escalated privileges by replacing the message with a specially crafted format string.

2) Another format string error exists in the alert notification process when displaying a notification message upon detection of a malicious file. This can be exploited to crash the Real Time Virus Scan service by replacing the message with a specially crafted format string.

References:
http://securityresponse.symantec.com/avcenter/security/Content/2006.09.13.html
http://layereddefense.com/SAV13SEPT.html

Cisco IOS VTP Multiple Vulnerabilities
“Denial of Service”

FX has reported some vulnerabilities in Cisco IOS, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially to compromise a vulnerable network device.

1) An error exists in the handling of summary packets in the VLAN Truncing Protocol (VTP). This can be exploited to reset the switch with a Software Forced Crash Exception by sending a specially crafted packet to a trunk enabled port.

2) An integer overflow error exists in the VTP configuration revision handling. This can be exploited to prevent that changes to the VLAN database are properly propagated throughout the VTP domain by sending a specially crafted packet containing 0x7FFFFFFF as a configuration revision number.

3) A boundary error exists in the processing of VTP summary advertisement messages. This can be exploited to cause a heap-based buffer overflow by sending a specially crafted message containing an overly long VLAN name (more than 100 characters) to a trunk enabled port.

Successful exploitation may allow arbitrary code execution.

NOTE: The packets must be received with a matching domain name and a matching VTP domain password (if configured).

The vulnerabilities affect Cisco IOS with a VTP Operating Mode as either "server" or "client".

References:
http://www.phenoelit.de/stuff/CiscoVTP.txt
http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml

Adobe Flash Player Multiple Vulnerabilities

“Execution of arbitrary code”

Multiple vulnerabilities have been reported in Adobe Flash Player, which can be exploited by malicious people to bypass certain security restrictions or compromise a user's system.

1) A boundary error during the handling of strings dynamically generated at runtime can be exploited to cause a buffer overflow via an overly long string.

Successful exploitation allows execution of arbitrary code when e.g. visiting a malicious website.

2) An unspecified error allows bypassing the "allowScriptAccess" option.

3) Using a "Shockwave Flash Object", it is possible to execute Flash files containing JavaScript embedded in Office documents automatically when the Office document is opened.

References:
http://www.adobe.com/support/security/bulletins/apsb06-11.html
http://www.computerterrorism.com/research/ct12-09-2006.htm
http://www.microsoft.com/technet/security/advisory/925143.mspx

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