netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 5

February 1, 2008

Table of Contents

Product Focus

Nimda Worm Scanner – The Nimda 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 MS IE Mime Header Flaw (MS01-020) or have been infected by the Nimda Worm.

Check out our video section for a number of interviews with Jesper Jurcenoks:
www.netvigilance.com/videos

This Week in Review

Interview with world's top security technologist. Enterprise forum to promote web 2.0 security awareness. Visa updates list of vendors who store card data improperly. Phishers control dns servers.

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

- **Talking security with Bruce Almighty**

When the good folk at Linux Australia sat down with the organisers of the Australian national Linux conference and decided that Bruce Schneier would be the keynote speaker on the opening day of the main conference, they couldn't have made a

more correct decision.
Schneier is a man whose security credentials are impeccable, who's probably the world's top security technologist. At the same time, he can talk about security concepts to a teenager - and the kid will understand exactly what he's saying.

When you realise that this same man is an inventor of the Blowfish, Twofish and Yarrow algorithms, then you begin to understand what the word intellectual means.

ITWire

Full Story :
http://www.itwire.com/content/view/16422/1090/

❖ Fortune 500 alliance targets web 2.0 security

In measure of its growing popularity in the business world, web 2.0 development has been boosted by the launch of a new large enterprise forum.
A newly launched forum of global corporations is aiming to promote awareness of secure use of web 2.0 technologies in the enterprise.

The Secure Enterprise 2.0 Forum held its inaugural event in London earlier this week, attracting a number of Fortune Global 500 executives and security experts to raise awareness define industry standards and best practices and facilitate interoperability for the secure use of web 2.0 technologies in the enterprise.

ITPro

Full Story :
http://www.itpro.co.uk/news/161610/fortune-500-alliance-targets-web-20-security.html

❖ Visa adds to its list of payment apps that improperly store card data

Update puts three more vendors on the list, according to a copy of the bulletin posted on the Web
Visa Inc. this week privately issued an updated list of payment applications that store all of the magnetic-stripe data taken from credit and debit cards, as part of its ongoing effort to get retailers and other merchants to stop using such software.

Visa began distributing the list last April and has updated it every three months since then. The company doesn't make the list openly available and hasn't publicly identified any of the vendors whose products are on it. Instead, Visa sends the list to so-called acquiring banks, the financial institutions that authorize merchants to accept payment-card transactions.

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9060538&taxonomyId=17&intsrc=kc_top

- **New phishing attacks use DNS tricks to dupe hapless users**

There's a sharp rise in malware that directs users to DNS (Domain Name System) servers controlled by phishers.
The latest information on phishing indicates that fraudsters are increasingly using malicious software to direct users to their deceptive sites.
The Anti-Phishing Working Group (APWG) said in a new report Thursday that it saw a sharp rise in November in malware that directs users to DNS (Domain Name System) servers controlled by phishers.

Business.ca

Full Story :
http://www.itbusiness.ca/it/client/en/home/news.asp?id=46967

New Vulnerabilities Tested in SecureScout

- **16843 QuickTime Multiple vulnerabilities in QuickTime for Java which may allow untrusted Java applets to obtain elevated privileges (Remote File Checking)**

Multiple vulnerabilities exist in QuickTime for Java, which may allow untrusted Java applets to obtain elevated privileges. By enticing a user to visit a web page containing a maliciously crafted Java applet, an attacker may cause the disclosure of sensitive information and arbitrary code execution with elevated privileges.

The issue has been fixed in version 7.3.0.

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

References:

* CONFIRM:
http://docs.info.apple.com/article.html?artnum=306896
* APPLE: APPLE-SA-2007-11-05
http://lists.apple.com/archives/Security-announce/2007/Nov/msg00000.html
* CERT: TA07-310A
http://www.us-cert.gov/cas/techalerts/TA07-310A.html
* CERT-VN: VU#319771
http://www.kb.cert.org/vuls/id/319771
* BID: 26339
http://www.securityfocus.com/bid/26339
* FRSIRT: ADV-2007-3723
http://www.frsirt.com/english/advisories/2007/3723
* SECTRACK: 1018894
http://www.securitytracker.com/id?1018894
* SECUNIA: 27523
http://secunia.com/advisories/27523
* XF: apple-quicktime-javaapplet-code-execution(38271)
http://xforce.iss.net/xforce/xfdb/38271

CVE Reference: CVE-2007-3751

❖ 16842 QuickTime heap buffer overflow in QuickTime Player's handling of Sample Table Sample Descriptor (STSD) atoms (Remote File Checking)

A heap buffer overflow exists in QuickTime Player's handling of Sample Table Sample Descriptor (STSD) atoms. By enticing a user to open a maliciously crafted movie file, an attacker may cause an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.3.0.

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

References:

* CONFIRM:
http://docs.info.apple.com/article.html?artnum=306896
* APPLE: APPLE-SA-2007-11-05
http://lists.apple.com/archives/Security-announce/2007/Nov/msg00000.html
* CERT: TA07-310A
http://www.us-cert.gov/cas/techalerts/TA07-310A.html
* BID: 26341
http://www.securityfocus.com/bid/26341
* FRSIRT: ADV-2007-3723
http://www.frsirt.com/english/advisories/2007/3723
* SECTRACK: 1018894
http://www.securitytracker.com/id?1018894
* SECUNIA: 27523
http://secunia.com/advisories/27523
* XF: apple-quicktime-stsd-atoms-bo(38268)
http://xforce.iss.net/xforce/xfdb/38268

CVE Reference: CVE-2007-3750

❖ 16841 QuickTime memory corruption issue in QuickTime's handling of image description atoms (Remote File Checking)

A memory corruption issue exists in QuickTime's handling of image description atoms. By enticing a user to open a maliciously crafted movie file, an attacker may cause an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.3.0.

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

References:

* CONFIRM:
http://docs.info.apple.com/article.html?artnum=306896
* APPLE: APPLE-SA-2007-11-05
http://lists.apple.com/archives/Security-announce/2007/Nov/msg00000.html
* CERT: TA07-310A
http://www.us-cert.gov/cas/techalerts/TA07-310A.html
* CERT-VN: VU#797875
http://www.kb.cert.org/vuls/id/797875
* BID: 26340
http://www.securityfocus.com/bid/26340
* FRSIRT: ADV-2007-3723
http://www.frsirt.com/english/advisories/2007/3723
* SECTRACK: 1018894
http://www.securitytracker.com/id?1018894
* SECUNIA: 27523
http://secunia.com/advisories/27523
* XF: apple-quicktime-movie-code-execution(38266)
http://xforce.iss.net/xforce/xfdb/38266

CVE Reference: CVE-2007-2395

❖ 16840 QuickTime vulnerabilities in QuickTime's Flash media handler (Remote File Checking)

Multiple vulnerabilities exist in QuickTime's Flash media handler, the most serious of which may lead to arbitrary code execution.

The issue has been fixed in version 7.3.1.

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

References:

* MISC:
http://docs.info.apple.com/article.html?artnum=307176
* APPLE: APPLE-SA-2007-12-13
http://lists.apple.com/archives/Security-announce/2007/Dec/msg00000.html
* BID: 26866
http://www.securityfocus.com/bid/26866
* FRSIRT: ADV-2007-4217
http://www.frsirt.com/english/advisories/2007/4217
* SECTRACK: 1019099
http://www.securitytracker.com/id?1019099
* SECUNIA: 28092
http://secunia.com/advisories/28092
* XF: quicktime-flash-media-code-execution(39030)
http://xforce.iss.net/xforce/xfdb/39030

CVE Reference: CVE-2007-4707

❖ 16839 QuickTime heap buffer overflow in QuickTime's handling of QTL files (Remote File Checking)

A heap buffer overflow exists in QuickTime's handling of QTL files. By enticing a user to view a maliciously crafted QTL file, an attacker may cause an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.3.1.

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

References:

* MISC:
http://docs.info.apple.com/article.html?artnum=307176
* APPLE: APPLE-SA-2007-12-13
http://lists.apple.com/archives/Security-announce/2007/Dec/msg00000.html
* BID: 26868
http://www.securityfocus.com/bid/26868
* FRSIRT: ADV-2007-4217
http://www.frsirt.com/english/advisories/2007/4217
* SECTRACK: 1019099
http://www.securitytracker.com/id?1019099
* SECUNIA: 28092
http://secunia.com/advisories/28092
* XF: quicktime-qtl-bo(39029)
http://xforce.iss.net/xforce/xfdb/39029

CVE Reference: CVE-2007-4706

❖ 16838 QuickTime buffer overflow in QuickTime's handling of Real Time Streaming Protocol (RTSP) headers (Remote File Checking)

A buffer overflow exists in QuickTime's handling of Real Time Streaming Protocol (RTSP) headers. By enticing a user to view a maliciously crafted RTSP movie, an attacker may cause an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.3.1.

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

References:

* MILW0RM: 4648
http://www.milw0rm.com/exploits/4648
* MISC:
http://www.beskerming.com/security/2007/11/25/74/QuickTime_-_Remote_hacker_automatic_control
* MISC:
http://docs.info.apple.com/article.html?artnum=307176
* APPLE: APPLE-SA-2007-12-13

http://lists.apple.com/archives/Security-announce/2007/Dec/msg00000.html
* CERT-VN: VU#659761
http://www.kb.cert.org/vuls/id/659761
* BID: 26549
http://www.securityfocus.com/bid/26549
* FRSIRT: ADV-2007-3984
http://www.frsirt.com/english/advisories/2007/3984
* SECTRACK: 1018989
http://www.securitytracker.com/id?1018989
* SECUNIA: 27755
http://secunia.com/advisories/27755
* XF: quicktime-rtsp-contenttype-bo(38604)
http://xforce.iss.net/xforce/xfdb/38604

CVE Reference: CVE-2007-6166

❖ 16837 QuickTime buffer overflow while processing a compressed PICT image (Remote File Checking)

A buffer overflow may occur while processing a compressed PICT image. Opening a maliciously crafted compressed PICT file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.4.0.

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

References:

* APPLE: APPLE-SA-2008-01-15
http://lists.apple.com/archives/security-announce/2008/Jan/msg00001.html
* CONFIRM:
http://docs.info.apple.com/article.html?artnum=307301
* CERT: TA08-016A
http://www.us-cert.gov/cas/techalerts/TA08-016A.html
* FRSIRT: ADV-2008-0148
http://www.frsirt.com/english/advisories/2008/0148
* SECTRACK: 1019221
http://www.securitytracker.com/id?1019221
* SECUNIA: 28502
http://secunia.com/advisories/28502
* XF: quicktime-pict-bo(39698)
http://xforce.iss.net/xforce/xfdb/39698

CVE Reference: CVE-2008-0036

❖ 16836 QuickTime memory corruption issue in QuickTime's parsing of Image Descriptor (IDSC) atoms (Remote File Checking)

A memory corruption issue exists in QuickTime's parsing of Image Descriptor (IDSC) atoms. Opening a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.4.0.

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

References:

* BUGTRAQ: 20080115 TPTI-08-01: Apple Quicktime Image File IDSC Atom Memory Corruption Vulnerability
http://www.securityfocus.com/archive/1/archive/1/486413/100/0/threaded
* MISC:
http://dvlabs.tippingpoint.com/advisory/TPTI-08-01
* APPLE: APPLE-SA-2008-01-15
http://lists.apple.com/archives/security-announce/2008/Jan/msg00001.html
* CONFIRM:
http://docs.info.apple.com/article.html?artnum=307301
* CERT: TA08-016A
http://www.us-cert.gov/cas/techalerts/TA08-016A.html
* FRSIRT: ADV-2008-0148
http://www.frsirt.com/english/advisories/2008/0148
* SECTRACK: 1019221
http://www.securitytracker.com/id?1019221
* SECUNIA: 28502
http://secunia.com/advisories/28502
* XF: quicktime-idsc-code-execution(39697)
http://xforce.iss.net/xforce/xfdb/39697

CVE Reference: CVE-2008-0033

❖ **16835 QuickTime memory corruption issue in QuickTime's handling of Macintosh Resource records in movie files (Remote File Checking)**

A memory corruption issue exists in QuickTime's handling of Macintosh Resource records in movie files. Opening a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.4.0.

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

References:

* IDEFENSE: 20080115 Apple QuickTime Macintosh Resource Processing Heap Corruption Vulnerability
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=642
* APPLE: APPLE-SA-2008-01-15
http://lists.apple.com/archives/security-announce/2008/Jan/msg00001.html
* CONFIRM:
http://docs.info.apple.com/article.html?artnum=307301
* CERT: TA08-016A
http://www.us-cert.gov/cas/techalerts/TA08-016A.html
* FRSIRT: ADV-2008-0148

http://www.frsirt.com/english/advisories/2008/0148
* SECTRACK: 1019221
http://www.securitytracker.com/id?1019221
* SECUNIA: 28502
http://secunia.com/advisories/28502
* XF: quicktime-macintosh-code-execution(39696)
http://xforce.iss.net/xforce/xfdb/39696

CVE Reference: CVE-2008-0032

❖ **16834 QuickTime memory corruption issue in QuickTime's handling of Sorenson 3 video files (Remote File Checking)**

A memory corruption issue exists in QuickTime's handling of Sorenson 3 video files. This may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.4.0.

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

References:

* APPLE: APPLE-SA-2008-01-15
http://lists.apple.com/archives/security-announce/2008/Jan/msg00001.html
* CONFIRM:
http://docs.info.apple.com/article.html?artnum=307301
* CERT: TA08-016A
http://www.us-cert.gov/cas/techalerts/TA08-016A.html
* FRSIRT: ADV-2008-0148
http://www.frsirt.com/english/advisories/2008/0148
* SECTRACK: 1019221
http://www.securitytracker.com/id?1019221
* SECUNIA: 28502
http://secunia.com/advisories/28502
* XF: quicktime-sorenson-code-execution(39695)
http://xforce.iss.net/xforce/xfdb/39695

CVE Reference: CVE-2008-0031

New Vulnerabilities found this Week

OpenBSD bgplg "cmd" Cross-Site Scripting Vulnerability
"conduct cross-site scripting attacks"

Alexandr Polyakov and Anton Karpov have reported a vulnerability in OpenBSD bgplg, which can be exploited by malicious people to conduct cross-site scripting attacks.

Input via the "cmd" parameter to the bgplg cgi-bin script is not properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script

code in a user's browser session in context of an affected site.

The vulnerability is reported in OpenBSD 4.1. OpenBSD 4.2 may also be affected.

References:
http://www.mail-archive.com/misc@openbsd.org/msg49057.html
http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/bgplg/bgplg.c

Cisco Wireless Control System Apache Tomcat JK Web Server Connector Buffer Overflow

"buffer overflow; code execution"

Cisco has acknowledged a vulnerability in Cisco Wireless Control System (WCS), which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability affects versions 3.x and 4.0.x prior to 4.0.100.0, and 4.1.x and 4.2.x prior to version 4.2.62.0.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20080130-wcs.shtml

Linux Kernel minix File System Denial of Service Vulnerability

"Denial of Service"

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

The vulnerability is caused due to improper handling of corrupted data structures in the minix file system. This can be exploited to crash a system by mounting a specially crafted image.

The vulnerability is reported in versions prior to 2.6.24.

Note: Several other issues, of which some may be security relevant, were also reported in the change log of version 2.6.24.

References:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.24

Cisco PIX and ASA Time-To-Live Denial of Service Vulnerability

"Denial of Service"

Cisco has acknowledged a vulnerability in Cisco PIX and ASA appliances, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an unspecified error in the processing of IP packets. This can be exploited to reload an affected device via specially crafted IP packets.

Successful exploitation requires that the Time-To-Live (TTL) decrement feature is enabled (disabled by default).

The vulnerability affects software versions 7.2(2) and later, prior to 7.2(3)006 or 8.0(3).

References:
http://www.cisco.com/warp/public/707/cisco-sa-20080123-asa.shtml

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