netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 10

March 9, 2007

Table of Contents

Product Focus

Mydoom Worm Scanner – The S4 MyDoom Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any have been infected by the MyDoom email virus or its variants.

This Week in Review

Online fraud shows up n court. Know the regulations. Security in database communications needs to be looked into. We must prioritize defending against cybercrime.

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

- **$3 Million Frozen in Cyber-Fraud Case**

A federal judge has frozen $3 million belonging to an Eastern European cyber-ring in an online stock manipulation case involving seven major brokerages, the largest asset freeze to date in such cases.

The ring's members lived in Russia, Latvia, Lithuania and the British Virgin Islands, and netted at least $733,000 from December 2005 to December 2006 in a complex

scheme that combined hacking with traditional "pump-and-dump" market manipulation, the Securities and Exchange Commission alleged in a complaint filed Tuesday in U.S. District Court in Washington.
Using a technique growing in popularity with cyber-criminals, the hackers cloaked their electronic footprints by hijacking the Internet protocol addresses of unrelated third parties across the United States, the SEC said yesterday.

Washingtonpost.com

Full Story :
http://www.washingtonpost.com/wp-dyn/content/article/2007/03/07/AR2007030702240.html

❖ Have you read your regulations?

Don't assume everything you're told is true when it comes to compliance specifics -- do your homework and find out what's legit and what's bull
I overheard a long-time hospital client talking to another support vendor today. The hospital's patient accounting department was attempting to send patient financial and billing data to a third-party biller. The vendor's normal Web site was down, and they were trying to come up with an emergency fix.

The pressing problem of the moment was how to securely transmit the data from the hospital to the third party. There are, of course, myriad options. The hospital clerk asked if she could e-mail the data file to the third-party vendor using a password-protected and encrypted Winzip file. The vendor's response was an emphatic and swift rejection. "Winzip encryption is not covered under HIPAA (Healthcare Insurance Portability Accountability Act) guidelines," said the vendor.

The week before, I heard a similar conversation with a national computer support person telling another client of mine that WEP wireless security isn't covered under the PCI (Payment Card Industry) Data Security Standard.

infoworld

Full Story :
http://www.infoworld.com/article/07/03/09/11OPsecadvise_1.html?source=rss&url=http://www.infoworld.com/article/07/03/09/11OPsecadvise_1.html

❖ Database security undermined by protocol loopholes and lax defences

A security expert is warning database administrators about a continued loophole in database communication protocols that would allow an attacker to bypass access controls and gain access to critical files.
In his presentation to attendees at the recent Black Hat DC training conference, Amichai Shulman, chief technology officer and founder of database-monitoring vendor Imperva explained that the client-server protocols, which are used to exchange data and commands between client software and database servers over TCP/IP, are ripe for attack.

The method can be used to victimize nearly all brands of database servers, including

IBM's DB2, Oracle Corp., and Microsoft's SQL Server. The loopholes allow an attacker to manipulate structured information and work below the radar of the database built-in mechanisms, Shulman said.

computerweekly

Full Story :
http://www.computerweekly.com/Articles/2007/03/06/222267/database-security-undermined-by-protocol-loopholes-and-lax.htm

- **Cybercrime must be a priority**

Not enough is being done to prevent low-level cyber-crime because it is not a priority to the police or Home Office, according to independent peer Lord Erroll.

Erroll told Microsoft's Architectural Insight Conference that cybercrime has been a contentious issue for some time and is not going away.

'E-Crime is climbing steadily, but it's not a Home Office or police priority,' said Erroll. 'There is a feeling that all we need to do is say use a firewall or anti-virus product and lock the doors of your data. This doesn't work. There is no ability to prosecute level two crimes where the amount lost is low because it is below the individual police area's radar.'

He urged resistance to proposals to water down the Data Protection Act.

'We need to resist this and make sure that it works. Chinese walls are useful but if we are going to use them we have to make sure they work,' he said.

Erroll says government wants to make personal information more widely available.

'The government wants to increase data sharing to make joined up government more efficient,' he said. 'Change your address once and it will ripple through the entire organisation. It has lots of benefits but huge dangers. Systems need to be able to handle those who are the exception and who do not want their address and data moved around.'

There is a danger that legislation passed on cybercrime is useless, because it's not enforced properly, according to Erroll.

Computerweekly.com

Full Story :
http://www.computerweekly.com/Articles/2007/03/06/222267/database-security-undermined-by-protocol-loopholes-and-lax.htm

New Vulnerabilities Tested in SecureScout

- **16449 QuickTime buffer overflow in the handling of 3GP video files (Remote File Checking)**

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

An integer overflow error exists in the handling of 3GP video files.

NOTE: This does not affect QuickTime on Mac OS X.

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

References:

Original Advisory:
APPLE-SA-2007-03-05
http://lists.apple.com/archives/Security-announce/2007/Mar/msg00000.html

Other references:
http://docs.info.apple.com/article.html?artnum=305149

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

CVE Reference: CVE-2007-0711

❖ 16450 QuickTime buffer overflow in the handling of MIDI files (Remote File Checking)

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

A boundary error in the handling of MIDI files can be exploited to cause a heap-based buffer overflow.

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

References:

Original Advisory:
APPLE-SA-2007-03-05
http://lists.apple.com/archives/Security-announce/2007/Mar/msg00000.html

Other references:
http://docs.info.apple.com/article.html?artnum=305149

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

CVE Reference: CVE-2007-0712

❖ 16451 QuickTime buffer overflow in the handling of QuickTime movie files (Remote File Checking)

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

A boundary error in the handling of QuickTime movie files can be exploited to cause a heap-based buffer overflow.

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

References:

Original Advisory:
APPLE-SA-2007-03-05
http://lists.apple.com/archives/Security-announce/2007/Mar/msg00000.html

Other references:
http://docs.info.apple.com/article.html?artnum=305149

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

CVE Reference: CVE-2007-0713

❖ 16452 QuickTime buffer overflow in the processing of UDTA atom size values in movie files (Remote File Checking)

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

An integer overflow exists in the processing of UDTA atom size values in movie files, which can be exploited to corrupt heap memory.

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

References:

Original Advisory:
APPLE-SA-2007-03-05
http://lists.apple.com/archives/Security-announce/2007/Mar/msg00000.html

Other references:
http://docs.info.apple.com/article.html?artnum=305149

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

CVE Reference: CVE-2007-0714

❖ 16453 QuickTime buffer overflow in the handling of PICT files (Remote File Checking)

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

A boundary error in the handling of PICT files can be exploited to cause a heap-based buffer overflow.

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

References:

Original Advisory:
APPLE-SA-2007-03-05
http://lists.apple.com/archives/Security-announce/2007/Mar/msg00000.html

Other references:
http://docs.info.apple.com/article.html?artnum=305149

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

CVE Reference: CVE-2007-0715

❖ 16454 QuickTime buffer overflow in the handling of QTIF files (Remote File Checking)

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

A boundary error in the handling of QTIF files can be exploited to cause a stack-based buffer overflow.

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

References:

Original Advisory:
APPLE-SA-2007-03-05
http://lists.apple.com/archives/Security-announce/2007/Mar/msg00000.html

Other references:
http://docs.info.apple.com/article.html?artnum=305149

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

CVE Reference: CVE-2007-0716

❖ 16455 QuickTime buffer overflow in the handling of QTIF files (Remote File Checking)

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

An integer overflow exists in the handling of QTIF files.

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

References:

Original Advisory:
APPLE-SA-2007-03-05
http://lists.apple.com/archives/Security-announce/2007/Mar/msg00000.html

Other references:
http://docs.info.apple.com/article.html?artnum=305149

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

CVE Reference: CVE-2007-0717

❖ 16456 QuickTime input validation error in the processing of QTIF files (Remote File Checking)

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

An input validation error exists in the processing of QTIF files. This can be exploited to cause a heap corruption via a specially crafted QTIF file with the "Color Table ID" field set to "0".

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

References:

Original Advisory:
APPLE-SA-2007-03-05
http://lists.apple.com/archives/Security-announce/2007/Mar/msg00000.html

Other references:
http://docs.info.apple.com/article.html?artnum=305149

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

CVE Reference: CVE-2007-0718

❖ 16457 Wireshark HTTP dissector Denial of Service Vulnerability (Remote File Checking)

Unspecified vulnerability in the HTTP dissector in Wireshark (formerly Ethereal) 0.99.3 allows remote attackers to cause a denial of service (crash) via unspecified vectors.

The vulnerability has been reported in version 0.99.3.

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

References:

Original Advisory:
http://www.wireshark.org/security/wnpa-sec-2006-03.html

Other references:
BUGTRAQ:20061101 rPSA-2006-0202-1 tshark wireshark
URL:http://www.securityfocus.com/archive/1/archive/1/450307/100/0/threaded
CONFIRM: https://issues.rpath.com/browse/RPL-746
CONFIRM: http://support.avaya.com/elmodocs2/security/ASA-2006-255.htm
MANDRIVA:MDKSA-2006:195
URL:http://www.mandriva.com/security/advisories?name=MDKSA-2006:195
REDHAT:RHSA-2006:0726
URL:http://www.redhat.com/support/errata/RHSA-2006-0726.html
SGI:20061101-01-P
URL:ftp://patches.sgi.com/support/free/security/advisories/20061101-01-P
SUSE:SUSE-SA:2006:065
URL:http://www.novell.com/linux/security/advisories/2006_65_ethereal.html
CERT-VN:VU#363992
URL:http://www.kb.cert.org/vuls/id/363992
BID:20762
URL:http://www.securityfocus.com/bid/20762
FRSIRT:ADV-2006-4220
URL:http://www.frsirt.com/english/advisories/2006/4220
SECTRACK:1017129
URL:http://securitytracker.com/id?1017129
SECUNIA:22590
URL:http://secunia.com/advisories/22590
SECUNIA:22692
URL:http://secunia.com/advisories/22692
SECUNIA:22672
URL:http://secunia.com/advisories/22672
SECUNIA:22797
URL:http://secunia.com/advisories/22797
SECUNIA:22841
URL:http://secunia.com/advisories/22841
SECUNIA:22929
URL:http://secunia.com/advisories/22929
SECUNIA:23096
URL:http://secunia.com/advisories/23096
XF:wireshark-http-dos(29840)
URL:http://xforce.iss.net/xforce/xfdb/29840

Product Homepage:
http://www.wireshark.org/

CVE Reference: CVE-2006-5468

❖ **16458 Wireshark LDAP dissector Denial of Service Vulnerability (Remote File Checking)**

Unspecified vulnerability in the LDAP dissector in Wireshark (formerly Ethereal) 0.99.3 allows remote attackers to cause a denial of service (crash) via a crafted LDAP packet.

The vulnerability has been reported in version 0.99.3.

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

References:

Original Advisory:
http://www.wireshark.org/security/wnpa-sec-2006-03.html

Other references:
BUGTRAQ:20061101 rPSA-2006-0202-1 tshark wireshark
#
URL:http://www.securityfocus.com/archive/1/archive/1/450307/100/0/threaded
CONFIRM: https://issues.rpath.com/browse/RPL-746
CONFIRM: http://support.avaya.com/elmodocs2/security/ASA-2006-255.htm
MANDRIVA:MDKSA-2006:195
URL:http://www.mandriva.com/security/advisories?name=MDKSA-2006:195
REDHAT:RHSA-2006:0726
URL:http://www.redhat.com/support/errata/RHSA-2006-0726.html
SGI:20061101-01-P
URL:ftp://patches.sgi.com/support/free/security/advisories/20061101-01-P
SUSE:SUSE-SA:2006:065
URL:http://www.novell.com/linux/security/advisories/2006_65_ethereal.html
BID:20762
URL:http://www.securityfocus.com/bid/20762
FRSIRT:ADV-2006-4220
URL:http://www.frsirt.com/english/advisories/2006/4220
SECTRACK:1017129
URL:http://securitytracker.com/alerts/2006/Oct/1017129.html
SECUNIA:22590
URL:http://secunia.com/advisories/22590
SECUNIA:22692
URL:http://secunia.com/advisories/22692
SECUNIA:22672
URL:http://secunia.com/advisories/22672
SECUNIA:22797
URL:http://secunia.com/advisories/22797
SECUNIA:22841
URL:http://secunia.com/advisories/22841
SECUNIA:22929
URL:http://secunia.com/advisories/22929
SECUNIA:23096
URL:http://secunia.com/advisories/23096
XF:wireshark-ldap-dos(29841)
URL:http://xforce.iss.net/xforce/xfdb/29841

Product Homepage:
http://www.wireshark.org/

CVE Reference: CVE-2006-5740

New Vulnerabilities found this Week

Apple QuickTime Multiple Vulnerabilities

"Code execution"

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

1) An integer overflow error exists in the handling of 3GP video files.

NOTE: This does not affect QuickTime on Mac OS X.

2) A boundary error in the handling of MIDI files can be exploited to cause a heap-based buffer overflow.

3) A boundary error in the handling of QuickTime movie files can be exploited to cause a heap-based buffer overflow.

4) An integer overflow exists in the processing of UDTA atom size values in movie files, which can be exploited to corrupt heap memory.

5) A boundary error in the handling of PICT files can be exploited to cause a heap-based buffer overflow.

6) A boundary error in the handling of QTIF files can be exploited to cause a stack-based buffer overflow.

7) An integer overflow exists in the handling of QTIF files.

8) An input validation error exists in the processing of QTIF files. This can be exploited to cause a heap corruption via a specially crafted QTIF file with the "Color Table ID" field set to "0".

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

References:
http://docs.info.apple.com/article.html?artnum=305149
http://descriptions.securescout.com/tc/16449
http://descriptions.securescout.com/tc/16450
http://descriptions.securescout.com/tc/16451
http://descriptions.securescout.com/tc/16452
http://descriptions.securescout.com/tc/16453
http://descriptions.securescout.com/tc/16454
http://descriptions.securescout.com/tc/16455
http://descriptions.securescout.com/tc/16456

Ipswitch IMail Server/Collaboration Suite IMAILAPI.DLL ActiveX Control Buffer Overflows

"Execution of arbitrary code"

Some vulnerabilities have been reported in Ipswitch IMail Server/Collaboration Suite,

which can be exploited by malicious people to compromise a vulnerable system.

The vulnerabilities are caused due to boundary errors within the IMAILAPI.DLL ActiveX control when processing WebConnect and Connect members of IMAILAPILib.IMailServer, Sync3 and Init3 of the IMAILAPILib.IMailLDAPService, and SetReplyTo of IMAILAPILib.IMailUserCollection. These can be exploited to cause various heap-based and stack-based buffer overflows when a user e.g. visits a specially crafted web site.

Successful exploitation allows execution of arbitrary code.

The vulnerabilities are reported in IMail Server 2006. Other versions may also be affected.

References:
http://www.ipswitch.com/support/ics/updates/ics20062.asp
http://support.ipswitch.com/kb/IM-20070305-JH01.htm

IBM DB2 Fenced UserID Directory Access Authentication Bypass
"Bypass authentication"

A security issue has been reported in IBM DB2, which can be exploited by malicious users to bypass certain security restrictions.

The security issue is due to an unspecified error and can be exploited to access certain directories without proper authentication.

References:
http://www-1.ibm.com/support/docview.wss?uid=swg1IY86711
http://www-1.ibm.com/support/docview.wss?uid=swg1IY87492

Mercury Mail Transport System IMAP Data Handling Buffer Overflow
"Execution of arbitrary code"

mu-b has discovered a vulnerability in Mercury Mail Transport System, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error when processing IMAP continuation data from the client. This can be exploited to cause a stack-based buffer overflow via a specially crafted series of commands and data sent to the IMAP service.

Successful exploitation allows execution of arbitrary code.

The vulnerability is reported in version 4.01b and confirmed in version 4.01a. Other versions may also be affected.

References:
http://lists.grok.org.uk/pipermail/full-disclosure/2007-March/052802.html

Asterisk SIP Message Handling Denial of Service
"Denial of Service"

MU Security Research Team has reported a vulnerability in Asterisk, which can be

exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to a NULL-pointer dereference error when handling SIP request messages. This can be exploited to crash the service via a specially crafted SIP message with no URI and SIP version sent to default port 5060/UDP.

The vulnerability is reported in version 1.4.0 and 1.2.15. Prior versions may also be affected.

References:
http://asterisk.org/node/48320
http://asterisk.org/node/48319

Adobe Reader and Acrobat PDF "file://" URL Handling Security Issue

"Disclose sensitive information"

pdp has discovered a security issue in Adobe Reader and Adobe Acrobat, which can be exploited by malicious people to disclose sensitive information.

The problem is that it is possible to launch "file://" URLs from within PDF files. This can be exploited to e.g. read arbitrary files on the system and send them to the attacker.

Successful exploitation requires that a user is tricked into locally opening a PDF file.

The security issue is confirmed in Adobe Reader and Adobe Acrobat Professional versions 8.0.0. Other versions may also be affected.

References:
http://www.gnucitizen.org/projects/pdf-strikes-back/

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