netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 1

January 5, 2007

Table of Contents

Product Focus

RPC DCOM Vulnerabilities Scanner – The RPC DCOM Vulnerabilities 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 Windows RPC DCOM flaws (MS03-026 and MS03-039).

netVigilance, Inc is proud to announce that we have been awarded the Payment Card Industry (PCI) Certifications as "Approved Scanning Vendor" (ASV).
This Certification allows netVigilance, Inc to determine PCI Data Security Standard (DSS) Compliance for vendors accepting Credit Cards on a worldwide basis.

This Week in Review

What about security in 2007? VoIP threatened. Bug in old pdf-reader. A different look at 2006.

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

- **10 things to know about info security in '07**

As I write this column, it is a balmy 55 degrees here in the Boston area--hardly the type of weather that drives New Englanders to start planning for the new year.

Nevertheless, the holidays have come and gone and it is thus time to take a stab at forecasting what to expect in information security over the next 12 months.

1. More privacy legislation
Now that the midterm elections are behind us, the folks in Washington will take a break from spending our money and focus on protecting our money. Democrats like Sens. Chuck Schumer of New York and Dianne Feinstein of California love this issue anyway and it makes good press--who wouldn't be in favor of cyber-protection for their constituencies? Look for a lot of grandstanding early in the year followed by the passing of a new data privacy bill sometime in the fall.

News.com

Full Story :
http://news.com.com/2010-7355_3-6147399.html?part=rss&tag=2547-1009_3-0-10&subj=news

❖ Voice over IP under threat

There has recently been considerable alarm about the possibility of a malicious code spreading via Skype. Skype is a system that allows voice communication over established Internet connections, in an environment very similar to that of telephone calls. It even allows calls to be made to telephones from a computer, with lower tariffs than that of a normal call.

The real problem that a malicious code for Voice over IP (VoIP) would suppose is that it opens a whole new field for hackers to create new types of malware. Initially, one might think of malicious code that uses VoIP in order to propagate, as was the case with the Trojan mentioned at the beginning. In reality, this represents nothing more than finding a new communication channel. New? No! There are already many worms that spread using numerous instant messaging systems. So this Trojan has not really done anything that hasn't been going on for many years now.

The problem lies in using the full characteristics of VoIP in order to spread malicious code. Imagine a dataflow across an audio channel (perhaps at a frequency that is not audible to humans) that could crash the voice system, causing a denial of service. Or that this dataflow could be used to create a system status that would allow execution of malicious code. This would be something genuinely new with respect to propagation of code, unlike other hundreds of codes that use messaging systems simply to propagate. But this is nothing more than speculation.

IT-Observer

Full Story :
http://www.it-observer.com/articles.php?id=1295

❖ Security bug found in PDF reader

Web users are being urged to upgrade their Adobe reader software as a security flaw is found in older versions of the program.

Millions of people use the reader software to view documents prepared in the popular PDF format.

Security researchers said malicious hackers exploiting the flaw could view victim's hard drives or use it to make phishing scams look more plausible.

So far there is no evidence that the bug is being exploited in the wild.

The flaw is found in the web browser plug-in of the Adobe Reader software. Ordinarily this allows PDF documents to be viewed in a browser window.

BBC News

Full Story :
http://news.bbc.co.uk/1/hi/technology/6234181.stm

- **Bud Broomhead and other great IT moments in 2006**

Most Awesome New Acronym of 2006: ARSE
Best IT Industry Name: Bud Broomhead. Not a cartoon character, but a real-life luck machine. Bud was a founding member of storage resource management pioneer HighGround Systems Inc., which was sold for a ton of money to Sun (see "Sun buys software firm HighGround"). Interestingly enough, HighGround was a Windows application, which I'm pretty sure you can't buy from Sun anymore. Bud then moved on to Topio Inc., which was just bought for another ton of money by NetApp.

Most Ridiculous Example of Starting and Selling Companies Ever: Rahul Mehta. First he did Manage-X, which he sold to HP, then Cluster-X, which he sold to Veritas, and now Storage-X (a marketing whiz he isn't, but who cares?) to Brocade. Even better, I'm not sure he ever did it with anyone else's money.

ComputerWorld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9007119&taxonomyId=17&intsrc=kc_feat

New Vulnerabilities Tested in SecureScout

- **14484 Adobe Acrobat / Reader Plug-in memory corruption and code execution Vulnerability (Remote File Checking)**

Stefano Di Paola and Giorgio Fedon have discovered a vulnerability in Adobe Reader which can be exploited to cause a memory corruption and potentially execution of arbitrary code.

Input passed to a hosted PDF file is not properly handled by the browser plug-in, which can be exploited to cause a memory corruption and potentially execution of arbitrary code.

The vulnerabilities are confirmed in version 6.0.1 for Windows via Internet Explorer 6 and version 7.0.8 for Windows via Firefox 2.0.0.1. Other versions may also be affected.

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

References:

Original advisories:
http://www.wisec.it/vulns.php?page=9

Other references:
http://www.kb.cert.org/vuls/id/815960
http://www.cert.org/advisories/CA-2000-02.html
http://events.ccc.de/congress/2006/Fahrplan/attachments/1158-Subverting_Ajax.pdf
http://www.wisec.it/vulns.php?page=9
http://secunia.com/advisories/23483/
http://www.adobe.com/devnet/acrobat/pdfs/PDFOpenParameters.pdf
http://en.wikipedia.org/wiki/Reverse_proxy

Product HomePage:
http://www.adobe.com/products/

CVE Reference:

❖ 14485 Adobe Acrobat / Reader Plug-in code execution Vulnerability (Remote File Checking)

Stefano Di Paola and Giorgio Fedon have discovered a vulnerability in Adobe Reader which can be exploited to execute arbitrary code.

Input passed to a hosted PDF file is not properly sanitized by the browser plug-in before being returned to users. This can be exploited to execute arbitrary script code in a user's browser session in context of an affected site.

The vulnerabilities are confirmed in version 6.0.1 for Windows via Internet Explorer 6 and version 7.0.8 for Windows via Firefox 2.0.0.1. Other versions may also be affected.

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

References:

Original advisories:
http://www.wisec.it/vulns.php?page=9

Other references:
http://www.kb.cert.org/vuls/id/815960
http://www.cert.org/advisories/CA-2000-02.html
http://events.ccc.de/congress/2006/Fahrplan/attachments/1158-Subverting_Ajax.pdf
http://www.wisec.it/vulns.php?page=9
http://secunia.com/advisories/23483/

http://www.adobe.com/devnet/acrobat/pdfs/PDFOpenParameters.pdf
http://en.wikipedia.org/wiki/Reverse_proxy

Product HomePage:
http://www.adobe.com/products/

CVE Reference:

❖ 14486 Adobe Acrobat / Reader Plug-in allows requesting arbitrary URLs Vulnerability (Remote File Checking)

Stefano Di Paola and Giorgio Fedon have discovered a vulnerability in Adobe Reader which can be exploited to allow requesting arbitrary URLs.

Input passed to a hosted PDF file is not properly sanitized by the browser plug-in and allows requesting arbitrary URLs, which provides a vector for performing CSRF attacks.

The vulnerabilities are confirmed in version 6.0.1 for Windows via Internet Explorer 6 and version 7.0.8 for Windows via Firefox 2.0.0.1. Other versions may also be affected.

The vulnerability has been reported in versions prior to 2.6.18.1.

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

References:

Original advisories:
http://www.wisec.it/vulns.php?page=9

Other references:
http://www.kb.cert.org/vuls/id/815960
http://www.cert.org/advisories/CA-2000-02.html
http://events.ccc.de/congress/2006/Fahrplan/attachments/1158-Subverting_Ajax.pdf
http://www.wisec.it/vulns.php?page=9
http://secunia.com/advisories/23483/
http://www.adobe.com/devnet/acrobat/pdfs/PDFOpenParameters.pdf
http://en.wikipedia.org/wiki/Reverse_proxy

Product HomePage:
http://www.adobe.com/products/

CVE Reference:

❖ 16384 Wireshark GSM BSSMAP dissector Denial of Service Vulnerabilities (Remote File Checking)

Unspecified vulnerability in Wireshark 0.10.11 to 0.99.0 allows remote attackers to cause a denial of service (abort) via the GSM BSSMAP dissector.

The vulnerabilities have been reported in versions 0.10.11 to 0.99.0.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00024.html

Other references:
BUGTRAQ:20060719 rPSA-2006-0132-1 tshark wireshark
#
URL:http://www.securityfocus.com/archive/1/archive/1/440576/100/0/threaded
CONFIRM: http://www.wireshark.org/security/wnpa-sec-2006-01.html
CONFIRM: https://issues.rpath.com/browse/RPL-512
CONFIRM: http://support.avaya.com/elmodocs2/security/ASA-2006-197.htm
GENTOO:GLSA-200607-09
URL:http://security.gentoo.org/glsa/glsa-200607-09.xml
MANDRIVA:MDKSA-2006:128
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:128
REDHAT:RHSA-2006:0602
URL:http://rhn.redhat.com/errata/RHSA-2006-0602.html
SGI:20060801-01-P
URL:ftp://patches.sgi.com/support/free/security/advisories/20060801-01-P
SUSE:SUSE-SR:2006:020
URL:http://www.novell.com/linux/security/advisories/2006_20_sr.html
BID:19051
URL:http://www.securityfocus.com/bid/19051
FRSIRT:ADV-2006-2850
URL:http://www.frsirt.com/english/advisories/2006/2850
SECUNIA:21078
URL:http://secunia.com/advisories/21078
SECUNIA:21107
URL:http://secunia.com/advisories/21107
SECUNIA:21121
URL:http://secunia.com/advisories/21121
SECUNIA:21204
URL:http://secunia.com/advisories/21204
SECUNIA:21488
URL:http://secunia.com/advisories/21488
SECUNIA:21598
URL:http://secunia.com/advisories/21598
SECUNIA:22089
URL:http://secunia.com/advisories/22089

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

CVE Reference: CVE-2006-3627

- **16385 Wireshark ANSI MAP, Checkpoint FW-1, MQ, XML, NTP dissectors Denial of Service and code execution Vulnerabilities (Remote File Checking)**

Multiple format string vulnerabilities in Wireshark (aka Ethereal) 0.10.x to 0.99.0 allow remote attackers to cause a denial of service and possibly execute arbitrary code via the (1) ANSI MAP, (2) Checkpoint FW-1, (3) MQ, (4) XML, and (5) NTP dissectors.

The vulnerabilities have been reported in versions 0.10.x to 0.99.0.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00024.html

Other references:
BUGTRAQ:20060719 rPSA-2006-0132-1 tshark wireshark
URL:http://www.securityfocus.com/archive/1/archive/1/440576/100/0/threaded
CONFIRM: http://www.wireshark.org/security/wnpa-sec-2006-01.html
CONFIRM: https://issues.rpath.com/browse/RPL-512
CONFIRM: http://support.avaya.com/elmodocs2/security/ASA-2006-197.htm
DEBIAN:DSA-1127
URL:http://www.debian.org/security/2006/dsa-1127
GENTOO:GLSA-200607-09
URL:http://security.gentoo.org/glsa/glsa-200607-09.xml
MANDRIVA:MDKSA-2006:128
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:128
REDHAT:RHSA-2006:0602
URL:http://rhn.redhat.com/errata/RHSA-2006-0602.html
SGI:20060801-01-P
URL:ftp://patches.sgi.com/support/free/security/advisories/20060801-01-P
SUSE:SUSE-SR:2006:020
URL:http://www.novell.com/linux/security/advisories/2006_20_sr.html
BID:19051
URL:http://www.securityfocus.com/bid/19051
FRSIRT:ADV-2006-2850
URL:http://www.frsirt.com/english/advisories/2006/2850
SECTRACK:1016532
URL:http://securitytracker.com/id?1016532
SECUNIA:21078
URL:http://secunia.com/advisories/21078
SECUNIA:21107
URL:http://secunia.com/advisories/21107
SECUNIA:21121
URL:http://secunia.com/advisories/21121
SECUNIA:21204
URL:http://secunia.com/advisories/21204
SECUNIA:21249
URL:http://secunia.com/advisories/21249
SECUNIA:21488
URL:http://secunia.com/advisories/21488
SECUNIA:21598
URL:http://secunia.com/advisories/21598

SECUNIA:22089
URL:http://secunia.com/advisories/22089

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

CVE Reference: CVE-2006-3628

❖ 16386 Wireshark MOUNT dissector Denial of Service Vulnerability (Remote File Checking)

Unspecified vulnerability in the MOUNT dissector in Wireshark (aka Ethereal) 0.9.4 to 0.99.0 allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors.

The vulnerabilities have been reported in versions 0.9.4 to 0.99.0.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00024.html

Other references:
BUGTRAQ:20060719 rPSA-2006-0132-1 tshark wireshark
URL:http://www.securityfocus.com/archive/1/archive/1/440576/100/0/threaded
CONFIRM: http://www.wireshark.org/security/wnpa-sec-2006-01.html
CONFIRM: https://issues.rpath.com/browse/RPL-512
CONFIRM: http://support.avaya.com/elmodocs2/security/ASA-2006-197.htm
DEBIAN:DSA-1127
URL:http://www.debian.org/security/2006/dsa-1127
GENTOO:GLSA-200607-09
URL:http://security.gentoo.org/glsa/glsa-200607-09.xml
MANDRIVA:MDKSA-2006:128
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:128
REDHAT:RHSA-2006:0602
URL:http://rhn.redhat.com/errata/RHSA-2006-0602.html
SGI:20060801-01-P
URL:ftp://patches.sgi.com/support/free/security/advisories/20060801-01-P
SUSE:SUSE-SR:2006:020
URL:http://www.novell.com/linux/security/advisories/2006_20_sr.html
BID:19051
URL:http://www.securityfocus.com/bid/19051
FRSIRT:ADV-2006-2850
URL:http://www.frsirt.com/english/advisories/2006/2850
SECTRACK:1016532
URL:http://securitytracker.com/id?1016532
SECUNIA:21078
URL:http://secunia.com/advisories/21078
SECUNIA:21107
URL:http://secunia.com/advisories/21107
SECUNIA:21121

URL:http://secunia.com/advisories/21121
SECUNIA:21204
URL:http://secunia.com/advisories/21204
SECUNIA:21249
URL:http://secunia.com/advisories/21249
SECUNIA:21488
URL:http://secunia.com/advisories/21488
SECUNIA:21598
URL:http://secunia.com/advisories/21598
SECUNIA:22089
URL:http://secunia.com/advisories/22089

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

CVE Reference: CVE-2006-3629

❖ 16387 Wireshark NCP NMAS and NDPS dissectors Denial of Service Vulnerability (Remote File Checking)

Multiple off-by-one errors in Wireshark (aka Ethereal) 0.9.7 to 0.99.0 have unknown impact and remote attack vectors via the (1) NCP NMAS and (2) NDPS dissectors.

The vulnerabilities have been reported in versions 0.9.7 to 0.99.0.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00024.html

Other references:
BUGTRAQ:20060719 rPSA-2006-0132-1 tshark wireshark
URL:http://www.securityfocus.com/archive/1/archive/1/440576/100/0/threaded
CONFIRM: http://www.wireshark.org/security/wnpa-sec-2006-01.html
CONFIRM: https://issues.rpath.com/browse/RPL-512
CONFIRM: http://support.avaya.com/elmodocs2/security/ASA-2006-197.htm
DEBIAN:DSA-1127
URL:http://www.debian.org/security/2006/dsa-1127
GENTOO:GLSA-200607-09
URL:http://security.gentoo.org/glsa/glsa-200607-09.xml
MANDRIVA:MDKSA-2006:128
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:128
REDHAT:RHSA-2006:0602
URL:http://rhn.redhat.com/errata/RHSA-2006-0602.html
SGI:20060801-01-P
URL:ftp://patches.sgi.com/support/free/security/advisories/20060801-01-P
SUSE:SUSE-SR:2006:020
URL:http://www.novell.com/linux/security/advisories/2006_20_sr.html
BID:19051
URL:http://www.securityfocus.com/bid/19051
FRSIRT:ADV-2006-2850

URL:http://www.frsirt.com/english/advisories/2006/2850
SECTRACK:1016532
URL:http://securitytracker.com/id?1016532
SECUNIA:21078
URL:http://secunia.com/advisories/21078
SECUNIA:21107
URL:http://secunia.com/advisories/21107
SECUNIA:21121
URL:http://secunia.com/advisories/21121
SECUNIA:21204
URL:http://secunia.com/advisories/21204
SECUNIA:21249
URL:http://secunia.com/advisories/21249
SECUNIA:21488
URL:http://secunia.com/advisories/21488
SECUNIA:21598
URL:http://secunia.com/advisories/21598
SECUNIA:22089
URL:http://secunia.com/advisories/22089

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

CVE Reference: CVE-2006-3630

❖ 16388 Wireshark SSH dissector Denial of Service Vulnerability (Remote File Checking)

Unspecified vulnerability in the SSH dissector in Wireshark (aka Ethereal) 0.9.10 to 0.99.0 allows remote attackers to cause a denial of service (infinite loop) via unknown attack vectors.

The vulnerabilities have been reported in versions 0.9.10 to 0.99.0.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00024.html

Other references:
BUGTRAQ:20060719 rPSA-2006-0132-1 tshark wireshark
URL:http://www.securityfocus.com/archive/1/archive/1/440576/100/0/threaded
CONFIRM: http://www.wireshark.org/security/wnpa-sec-2006-01.html
CONFIRM: http://support.avaya.com/elmodocs2/security/ASA-2006-197.htm
DEBIAN:DSA-1127
URL:http://www.debian.org/security/2006/dsa-1127
GENTOO:GLSA-200607-09
URL:http://security.gentoo.org/glsa/glsa-200607-09.xml
MANDRIVA:MDKSA-2006:128
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:128
REDHAT:RHSA-2006:0602
URL:http://rhn.redhat.com/errata/RHSA-2006-0602.html

SGI:20060801-01-P
URL:ftp://patches.sgi.com/support/free/security/advisories/20060801-01-P
SUSE:SUSE-SR:2006:020
URL:http://www.novell.com/linux/security/advisories/2006_20_sr.html
BID:19051
URL:http://www.securityfocus.com/bid/19051
FRSIRT:ADV-2006-2850
URL:http://www.frsirt.com/english/advisories/2006/2850
SECTRACK:1016532
URL:http://securitytracker.com/id?1016532
SECUNIA:21078
URL:http://secunia.com/advisories/21078
SECUNIA:21107
URL:http://secunia.com/advisories/21107
SECUNIA:21121
URL:http://secunia.com/advisories/21121
SECUNIA:21204
URL:http://secunia.com/advisories/21204
SECUNIA:21249
URL:http://secunia.com/advisories/21249
SECUNIA:21488
URL:http://secunia.com/advisories/21488
SECUNIA:21598
URL:http://secunia.com/advisories/21598
SECUNIA:22089
URL:http://secunia.com/advisories/22089

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

CVE Reference: CVE-2006-3631

❖ 16389 Wireshark NFS dissector Denial of Service and code execution Vulnerability (Remote File Checking)

Buffer overflow in Wireshark (aka Ethereal) 0.8.16 to 0.99.0 allows remote attackers to cause a denial of service and possibly execute arbitrary code via the NFS dissector.

The vulnerabilities have been reported in versions 0.8.16 to 0.99.0.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00024.html

Other references:
BUGTRAQ:20060719 rPSA-2006-0132-1 tshark wireshark
URL:http://www.securityfocus.com/archive/1/archive/1/440576/100/0/threaded
CONFIRM: http://www.wireshark.org/security/wnpa-sec-2006-01.html
CONFIRM: https://issues.rpath.com/browse/RPL-512

CONFIRM: http://support.avaya.com/elmodocs2/security/ASA-2006-197.htm
DEBIAN:DSA-1127
URL:http://www.debian.org/security/2006/dsa-1127
GENTOO:GLSA-200607-09
URL:http://security.gentoo.org/glsa/glsa-200607-09.xml
MANDRIVA:MDKSA-2006:128
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:128
REDHAT:RHSA-2006:0602
URL:http://rhn.redhat.com/errata/RHSA-2006-0602.html
SGI:20060801-01-P
URL:ftp://patches.sgi.com/support/free/security/advisories/20060801-01-P
SUSE:SUSE-SR:2006:020
URL:http://www.novell.com/linux/security/advisories/2006_20_sr.html
BID:19051
URL:http://www.securityfocus.com/bid/19051
FRSIRT:ADV-2006-2850
URL:http://www.frsirt.com/english/advisories/2006/2850
SECTRACK:1016532
URL:http://securitytracker.com/id?1016532
SECUNIA:21078
URL:http://secunia.com/advisories/21078
SECUNIA:21107
URL:http://secunia.com/advisories/21107
SECUNIA:21121
URL:http://secunia.com/advisories/21121
SECUNIA:21204
URL:http://secunia.com/advisories/21204
SECUNIA:21249
URL:http://secunia.com/advisories/21249
SECUNIA:21488
URL:http://secunia.com/advisories/21488
SECUNIA:21598
URL:http://secunia.com/advisories/21598
SECUNIA:22089
URL:http://secunia.com/advisories/22089

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

CVE Reference: CVE-2006-3632

❖ 16390 Wireshark DHCP dissector Denial of Service Vulnerability (Remote File Checking)

Unspecified vulnerability in the DHCP dissector in Wireshark (formerly Ethereal) 0.10.13 through 0.99.2, when run on Windows, allows remote attackers to cause a denial of service (crash) via unspecified vectors that trigger a bug in Glib.

The vulnerabilities have been reported in versions 0.10.13 through 0.99.2.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00024.html

Other references:
CONFIRM: http://www.wireshark.org/security/wnpa-sec-2006-02.html
GENTOO:GLSA-200608-26
URL:http://security.gentoo.org/glsa/glsa-200608-26.xml
MANDRIVA:MDKSA-2006:152
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:152
CERT-VN:VU#335656
URL:http://www.kb.cert.org/vuls/id/335656
BID:19690
URL:http://www.securityfocus.com/bid/19690
FRSIRT:ADV-2006-3370
URL:http://www.frsirt.com/english/advisories/2006/3370
SECTRACK:1016736
URL:http://securitytracker.com/id?1016736
SECUNIA:21597
URL:http://secunia.com/advisories/21597
SECUNIA:21649
URL:http://secunia.com/advisories/21649
SECUNIA:21619
URL:http://secunia.com/advisories/21619
SECUNIA:21682
URL:http://secunia.com/advisories/21682
XF:wireshark-dhcp-dos(28554)
URL:http://xforce.iss.net/xforce/xfdb/28554
XF:wireshark-esp-offbyone(28553)
URL:http://xforce.iss.net/xforce/xfdb/28553

Product Homepage:

CVE Reference: CVE-2006-4332

New Vulnerabilities found this Week

Apple Quicktime RTSP URL Handling Buffer Overflow Vulnerability

"Execution of arbitrary code"

LMH has discovered a vulnerability in Apple Quicktime, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error when handling RTSP URLs. This can be exploited to cause a stack-based buffer overflow via a specially crafted QTL file with an overly long (more than 256 bytes) "src" parameter (e.g. "rtsp://[any character]:[>256 bytes]").

Successful exploitation allows execution of arbitrary code and requires that the user is e.g. tricked into opening a malicious QTL file or visiting a malicious web site.

The vulnerability is confirmed in version 7.1.3.100 (Windows version) and reportedly affects both Microsoft Windows and Mac OS X versions.

References:
http://projects.info-pull.com/moab/MOAB-01-01-2007.html
http://www.kb.cert.org/vuls/id/442497

OpenOffice WMF/EMF Integer Overflow Vulnerability

"Execution of arbitrary code"

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

The vulnerability is caused due to integer overflows within the processor for WMF/EMF files. This can be exploited to cause a heap-based buffer overflow by e.g. tricking a user into opening a specially crafted WMF/EMF file.

Successful exploitation may allow the execution of arbitrary code.

References:
http://www.openoffice.org/issues/show_bug.cgi?id=70042

OpenBSD "vga" Privilege Escalation Vulnerability

"Gain escalated privileges"

A vulnerability has been reported in OpenBSD, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to an input validation error in sys/dev/pci/vga_pci.c of "vga" (VGA graphics driver for wscons), which can be exploited to gain escalated privileges.

Successful exploitation may allow to gain root privileges, but requires that the kernel is compiled with "option PCIAGP" (by default only available for i386) and that the device is not AGP compatible.

The vulnerability is reported in OpenBSD 3.9 and 4.0. Other versions may also be affected.
References:
http://www.openbsd.org/errata.html#agp

Adobe Reader Multiple Vulnerabilities

"Cross-site scripting attacks; code execution;"

Stefano Di Paola and Giorgio Fedon have discovered some vulnerabilities in Adobe Reader, which can be exploited by malicious people to conduct cross-site scripting attacks, as a vector for conducting cross-site request forgery attacks, or potentially compromise a user's system.

1) Input passed to a hosted PDF file is not properly handled by the browser plug-in, which can be exploited to cause a memory corruption and potentially execution of arbitrary code.

2) Input passed to a hosted PDF file is not properly sanitised by the browser plug-in before

being returned to users. This can be exploited to execute arbitrary script code in a user's browser session in context of an affected site.

3) Input passed to a hosted PDF file is not properly sanitised by the browser plug-in and allows requesting arbitrary URLs, which provides a vector for performing CSRF attacks.

It is also possible to cause the browser to stop responding by passing a lot of "#" characters.

The vulnerabilities are confirmed in version 6.0.1 for Windows via Internet Explorer 6 and version 7.0.8 for Windows via Firefox 2.0.0.1. Other versions may also be affected.

References:
http://www.wisec.it/vulns.php?page=9
http://www.kb.cert.org/vuls/id/815960
http://descriptions.securescout.com/tc/14484
http://descriptions.securescout.com/tc/14485
http://descriptions.securescout.com/tc/14486

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