netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 22

June 8, 2007

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.

This Week in Review

This week netVigilance Security Research has found 4 vulnerabilities in open source software MyEvent and DGNews:

1 high risk, 1 medium risk and 2 low risk. The vulnerabilities include SQL Injection, XSS (Cross site Scripting) and Path Disclosure Vulnerabilities.

To see details and further information please see:
http://www.netvigilance.com/advisories

Do faster chips make us right-wing? Security and privacy: Can they coexist? Retailers unsatisfied with PCI. Europe launches security standards.

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

❖ Perspective: Could Karl Rove be right about tech?

In an illuminating interview published in the June 4 issue of The New Yorker, White House political aide Karl Rove suggested that a nexus exists between the spread of technology and a centrist-conservative outlook on the world.

"There are two or three societal trends that are driving us in an increasingly deep center-right posture," Rove told the magazine. "One of them is the power of the computer chip. Do you know how many people's principal source of income is eBay? Seven hundred thousand."

Rove's point being that the proliferation of technology puts increasing numbers of people in charge of how they make a living.

He continues: "It's given people a greater chance to run their own business, become a sole proprietor or an entrepreneur. As a result, it has made us more market-oriented, and that equals making you more center-right in your politics."

c-net News

Full Story :
http://news.com.com/Could+Karl+Rove+be+right+about+tech/2010-1028_3-6189538.html?tag=newsmap

❖ The security solution revolution

Truly stopping malicious hackers and malware requires ubiquitous authentication for all users and devices. Are you in?
“Every generation needs a new revolution.” — Thomas Jefferson
A friend of mine recently sent me a link to the Department of Homeland Security’s request for proposals and whitepapers to address various cybersecurity topics. I applaud the government for actively encouraging new defense methods. However, I’m convinced that most of the proposals will not provide a lasting defense.

No matter what cool idea or whiz-bang way of detecting worms and bot nets comes out of the proposals, malicious hackers and computer malware will continue unabated. That’s because we continue to address symptoms and not the real, underlying problem. I’ve written about this before, but it bears repeating every so often so that my new readers understand how all the feel-good ideas in the world won’t make bad cyberguys go away.

If you want to stop malicious hackers and malware, you must create a new computing ecosystem where every device, user, process, transaction, and network packet is authenticated from source to destination. It means creating a new Internet, one where default anonymity is no longer guaranteed. In fact, a secure Internet would ensure that everyone and everything has a confirmed identity and can be authenticated and tracked.

infoworld

Full Story :
http://www.infoworld.com/article/07/06/08/23OPsecadvise_1.html?source=rss&url=http://www.infoworld.com/article/07/06/08/23OPsecadvise_1.html

❖ Retailers fume over PCI security rules

Claim credit card firms shift burden to them
Several retailers this week bristled at having to comply with the Payment Card Industry (PCI) Data Security Standard, complaining that they carry an unfair burden in securing credit card data.

In interviews and speeches at the annual ERIexchange retail event here, executives also complained that implementing the standards is costly and could alienate customers.

The companies face heavy fines and increased transaction rates for noncompliance with the PCI standards.

Steve Methvin, director of store systems at Bi-Lo LLC, a Greenville, S.C.-based grocery chain of about 230 stores in the southeastern U.S., called on the credit card companies themselves to do more to make cards more secure — such as adding a PIN.

He said that the credit card companies have declined to take such steps in order to avoid complaints from customers.

computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=government&articleId=9023998&taxonomyId=13&intsrc=kc_top

❖ ICT Security Standards Roadmap launches

Europe gets UN IT-security website portal
IT security specifications and standards organisations in Europe now have a a one-stop source for standards information. The ICT Security Standards Roadmap, is part of the website of the ITU (International Telecommunications Union), the telecommunications agency of the United Nations.

It is the first effort to create a repository for network and information security standardisation efforts in Europe for security vendors, service providers, developers and researchers, according to the ITU.

The portal lists standards organisations and specifications throughout Europe. The ICT Security Standards Roadmap will eventually detail ongoing projects between different standards bodies.

Contributors to the portal include the European Network and Information Security Agency and the Network and Information Security Steering Group, part of the ICT Standards Board.

Pc advisor

Full Story :
http://www.pcadvisor.co.uk/news/index.cfm?newsid=9638

New Vulnerabilities Tested in SecureScout

- **16514 Microsoft Internet Explorer Spoofing Vulnerability (Remote File Checking)**

Michal Zalewski has reported a vulnerability in Internet Explorer, which potentially can be exploited by a malicious website to spoof the URL address bar.

An error within the handling of "location" DOM objects can be exploited to spoof the URL address bar.

The vulnerability has been reported in all versions of Internet explorer 6.

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

References:

Original advisory:
http://lists.grok.org.uk/pipermail/full-disclosure/2007-June/063712.html

Other references:
http://www.kb.cert.org/vuls/id/471361

Product HomePage:
http://www.microsoft.com/windows/ie/default.asp

CVE Reference:

- **16513 Microsoft Internet Explorer race condition Vulnerability (Remote File Checking)**

Michal Zalewski has reported a vulnerability in Internet Explorer, which potentially can be exploited by a malicious website to bypass certain security restrictions.

A race condition when navigating to a new site from a page can be exploited to perform certain actions and access the contents of the newly loaded page with the permissions of the old page.

The vulnerability has been reported in all versions of Internet explorer 6 and 7.

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

References:

Original advisory:

http://lists.grok.org.uk/pipermail/full-disclosure/2007-June/063712.html

Other references:
http://www.kb.cert.org/vuls/id/471361

Product HomePage:
http://www.microsoft.com/windows/ie/default.asp

CVE Reference:

- **16512 QuickTime handling of Java applets, Information Disclosure Vulnerability (Remote File Checking)**

A vulnerability has been reported in Apple QuickTime, which can be exploited by malicious people to gain knowledge of potentially sensitive information.

A design error within the handling of Java applets can be exploited to read the browser's memory when a user visits a malicious website containing a malicious Java applet.

The issue has been fixed in version 7.1.6.

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

References:

Original Advisory:
APPLE-SA-2007-05-29
http://lists.apple.com/archives/security-announce/2007/May/msg00005.html

Other references:
CERT-VN:VU#995836
URL:http://www.kb.cert.org/vuls/id/995836
BID:24221
URL:http://www.securityfocus.com/bid/24221
FRSIRT:ADV-2007-1974
URL:http://www.frsirt.com/english/advisories/2007/1974
SECTRACK:1018136
URL:http://www.securitytracker.com/id?1018136
SECUNIA:25130
URL:http://secunia.com/advisories/25130

Product:
http://www.apple.com/quicktime/**CVE Reference:** CVE-2007-2388

- **16511 QuickTime QTObject, reading and writing of arbitrary memory Vulnerability (Remote File Checking)**

A vulnerability has been reported in Apple QuickTime, which can be exploited by malicious people to gain knowledge of potentially sensitive information or execute

arbitrary code.

A design error in the security restrictions on subclasses of QTObject can be exploited by untrusted Java code to allow subclassing of QuickTime objects that call unsafe functions from QTJava.dll resulting in reading and writing of arbitrary memory.

Successful exploitation allows execution of arbitrary code on Windows and OS X systems when a user visits a malicious web site using a Java-enabled browser.

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

References:

Original Advisory:
APPLE-SA-2007-05-29
http://lists.apple.com/archives/security-announce/2007/May/msg00005.html

Other references:
CERT-VN:VU#434748
URL:http://www.kb.cert.org/vuls/id/434748
BID:24222
URL:http://www.securityfocus.com/bid/24222
FRSIRT:ADV-2007-1974
URL:http://www.frsirt.com/english/advisories/2007/1974
SECTRACK:1018136
URL:http://www.securitytracker.com/id?1018136
SECUNIA:25130
URL:http://secunia.com/advisories/25130

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

CVE Reference: CVE-2007-2389

❖ 15437 Yahoo! Messenger ywcvwr.dll buffer overflow Vulnerability (Remote File Checking)

Yahoo! Messenger is a free instant messaging software.

Danny has discovered a vulnerability in Yahoo! Messenger, which can be exploited by malicious people to compromise a user's system.

A boundary error within the Yahoo! Webcam Viewer (ywcvwr.dll) ActiveX control can be exploited to cause a stack-based buffer overflow by assigning an overly long string to the "Server" property and then calling the "Receive()" method.

Successful exploitation of the vulnerability allows execution of arbitrary code.

The vulnerabilities are confirmed in version 8.1.0.249. Other versions may also be affected.

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

References:

Original Advisory:
http://lists.grok.org.uk/pipermail/full-disclosure/2007-June/063819.html

Other references:
N.A.

Vendor URL:
http://messenger.yahoo.com/

CVE Reference:

❖ 15298 Yahoo! Messenger ywcupl.dll buffer overflow Vulnerability (Remote File Checking)

-based buffer overflow by assigning an overly long string to the "Server" property and then calling the "Send()" method.

Successful exploitation of the vulnerability allows execution of arbitrary code.

The vulnerabilities are confirmed in version 8.1.0.249. Other versions may also be affected.

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

References:

Original Advisory:
http://lists.grok.org.uk/pipermail/full-disclosure/2007-June/063817.html

Other references:
N.A.

Vendor URL:
http://messenger.yahoo.com/

CVE Reference:

❖ 13542 Oracle Database Server - Upgrade/Downgrade component Buffer Overflow Vulnerability (apr-2007/DB13)

A buffer overflow vulnerability exists in Oracle Database Server Upgrade/Downgrade component.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-

updates/cpuapr2007.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2007-2118

❖ 13541 Oracle Database Server - Oracle Text component Buffer Overflow Vulnerability (apr-2007/DB12)

A buffer overflow vulnerability exists in Oracle Database Server Oracle Text component.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2007-2117

❖ 13540 Oracle Database Server - Oracle Instant Client component Buffer Overflow Vulnerability (apr-2007/DB11)

A buffer overflow vulnerability exists in Oracle Database Server Oracle Instant Client component.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2007-2114

- **13539 Oracle Database Server - Advanced Replication component Buffer Overflow Vulnerability (apr-2007/DB10)**

A buffer overflow vulnerability exists in Oracle Database Server Advanced Replication component.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2007-2116

New Vulnerabilities found this Week

Yahoo! Messenger Two ActiveX Controls Buffer Overflows
"Execution of arbitrary code"

Danny has discovered two vulnerabilities in Yahoo! Messenger, which can be exploited by malicious people to compromise a user's system.

1) A boundary error within the Yahoo! Webcam Upload (ywcupl.dll) ActiveX control can be exploited to cause a stack-based buffer overflow by assigning an overly long string to the "Server" property and then calling the "Send()" method.

2) A boundary error within the Yahoo! Webcam Viewer (ywcvwr.dll) ActiveX control can be exploited to cause a stack-based buffer overflow by assigning an overly long string to the "Server" property and then calling the "Receive()" method.

Successful exploitation of the vulnerabilities allows execution of arbitrary code.

The vulnerabilities are confirmed in version 8.1.0.249. Other versions may also be affected.

References:
http://lists.grok.org.uk/pipermail/full-disclosure/2007-June/063817.html
http://lists.grok.org.uk/pipermail/full-disclosure/2007-June/063819.html
http://descriptions.securescout.com/tc/15298
http://descriptions.securescout.com/tc/15437

Apple QuickTime Java Extension Two Vulnerabilities

"Reading and writing of arbitrary memory"

Two vulnerabilities have been reported in Apple QuickTime, which can be exploited by malicious people to gain knowledge of potentially sensitive information or compromise a user's system.

1) A design error in the security restrictions on subclasses of QTObject can be exploited by untrusted Java code to allow subclassing of QuickTime objects that call unsafe functions from QTJava.dll resulting in reading and writing of arbitrary memory.

Successful exploitation allows execution of arbitrary code on Windows and OS X systems when a user visits a malicious web site using a Java-enabled browser.

2) A design error within the handling of Java applets can be exploited to read the browser's memory when a user visits a malicious website containing a malicious Java applet.

References:
http://docs.info.apple.com/article.html?artnum=305531
http://www.kb.cert.org/vuls/id/434748
http://www.kb.cert.org/vuls/id/995836
http://descriptions.securescout.com/tc/16511
http://descriptions.securescout.com/tc/16512

Internet Explorer Page Loading Race Condition and URL Spoofing

"Fake URL in the address bar; Bypass security restrictions"

Michal Zalewski has reported two vulnerabilities in Internet Explorer, which potentially can be exploited by a malicious website to display a fake URL in the address bar or to bypass certain security restrictions.

1) A race condition when navigating to a new site from a page can be exploited to perform certain actions and access the contents of the newly loaded page with the permissions of the old page.

2) An error within the handling of "location" DOM objects can be exploited to spoof the URL address bar.

Note: This issue reportedly does not affect Internet Explorer 7.

References:
http://lists.grok.org.uk/pipermail/full-disclosure/2007-June/063712.html
http://descriptions.securescout.com/tc/16513
http://descriptions.securescout.com/tc/16514

Amavis file Integer Underflow and Denial of Service

"Denial of Service"

A vulnerability and a security issue have been reported in Amavis, which can be exploited by malicious people to cause a DoS (Denial of Service) or potentially to

compromise a vulnerable system.

1) An integer underflow error in the "file" utility can be exploited to cause a heap-based buffer overflow.

2) The problem is caused due to certain regular expressions in "file", which can consume all available CPU resources when identifying a specially crafted file.

References:
http://www.amavis.org/security/asa-2007-3.txt

CA Anti-Virus Engine CAB Archive Processing Buffer Overflows

"Execution of arbitrary code"

Two vulnerabilities have been reported in the CA Anti-Virus engine, which can be exploited by malicious people to compromise a vulnerable system.

1) A boundary error in vete.dll when processing CAB archives can be exploited to cause a stack-based buffer overflow via a specially crafted CAB archive containing overly long filenames.

2) An input validation error when processing the "coffFiles" field in CAB archives can be exploited to cause a stack-based buffer overflow.

Successful exploitation of the vulnerabilities allows execution of arbitrary code.

References:
http://supportconnectw.ca.com/public/antivirus/infodocs/caantivirus-securitynotice.asp

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