netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 30

August 3, 2007

Table of Contents

Product Focus

CodeRed Worm Scanner – The CodeRed 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 CodeRed Worm.

This Week in Review

A new generation of crimeware. Rootkkits not the only threat. Security researcers start billing vendors for vulnerabilities found. Hackers getting more organized.

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

- **When trojans go phishing**

Stealthy software more dangerous than ever
A new generation of so-called crimeware (crime software) is being used to steal banking customer data from infected PCs, according to a report by Finjan, a provider of secure web gateway products.

During July, Finjan claims, the firm identified 58 criminals using the MPack toolkit to

successfully infect over 500,000 users. Out of 3.1 million attempts at infecting PCs, 16% succeeded – indicated by the web traffic volumes of the infecting sites.

Analysis indicates that the crimeware being used within MPack steals bank account information, including user name, password, credit card numbers, and social security numbers in what Finjan describes as "a creative way."

Techcentral.ie

Full Story :
http://www.techcentral.ie/corporate_it/Trojan_phishing_Finjan/view

- **Researchers warn that rootkits aren't the only threat**

Other stealth techniques are equally effective -- and more imminent
Rootkits may be getting most of the attention within the security community. But it's important not to overlook other, equally effective antiforensic techniques that malware writers have at their disposal for hiding their code from detection, according to a security researcher at the Black Hat 2007 conference.

Nick Harbour, a senior consultant at Alexandria, Va.-based security vendor Mandiant, outlined a few of those techniques during a presentation at the show. None of the methods are especially new, but they have been only scarcely documented.

One of the ways in which malware writers can hide their code from forensic discovery is via a method known as process injection. The technique involves the injection of malicious code into another legitimate running process on an end user's system, Harbour said, speaking with Computerworld after his presentation.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9028858&taxonomyId=17&intsrc=kc_top

- **Bug hunting start-up: Pay up, or feel the pain**

An upstart security research firm with a controversial business model is at the center of a debate over how software bugs should be disclosed.
Vulnerability Discovery and Analysis (VDA) Labs, founded in April by Jared DeMott, notifies software vendors of security bugs found in their software, as do many other security researchers.

But as part of VDA's business model, vendors are asked to pay for the bugs it discovers, or its consulting services, otherwise VDA threatens to sell the bug to a third party or make the details of the security flaw public.

DeMott, who has done work for the National Security Agency among other places, describes his business model as "edgy," while other security researchers see it as more akin to "extortion." The practice, in either case, veers from the more traditional ways bug hunters have worked with software vendors and security firms.

Cnet news

Full Story :
http://news.com.com/Bug+hunting+start-up+Pay+up%2C+or+feel+the+pain/2100-7350_3-6200489.html?tag=cd.top

- **Corporates wrestle with growing global hacker threat**

The modern digital security arena sounds more like a cyber Olympics, with terms such as phishers, key loggers and Trojan horses, than a serious personal and corporate threat. But that is exactly what it is, says Ed MacNair, CEO of Marshal, the e-mail and Internet security company.
Targeted attacks proliferate today, and corporates find themselves in the trenches. Back in the '90s, the most common threat was viruses, and those were typically written by students showing off. They were the equivalent of a CV or résumé. Script kiddies arose from that culture. Script kiddie is a derogatory term in hacker culture used to describe inexperienced, malicious crackers who use other people's programs to attack computer systems.

The big change in the past two to three years has been the organisation of the cyber underworld. Criminal gangs have surfaced. For example, Amsterdam police recently arrested 111 people as part of Operation Apollo and a seven-month long investigation into Internet fraud. They believe up to 2000 people are involved in Internet fraud in the country.

Itc world

Full Story :
http://www.ictworld.co.za/EditorialEdit.asp?EditorialID=29507

New Vulnerabilities Tested in SecureScout

- **16565 QuickTime design issue may allow a malicious website to capture a client's screen content (Remote File Checking)**

A design issue exists in QuickTime for Java, which may allow a malicious website to capture a client's screen content. By enticing a user to visit a web page containing a

maliciously crafted Java applet, an attacker can trigger the issue which may lead to the disclosure of sensitive information.

The issue has been fixed in Firefox 2.0.0.5.

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

References:

* CONFIRM:
http://docs.info.apple.com/article.html?artnum=305947
* APPLE: APPLE-SA-2007-07-11
http://lists.apple.com/archives/Security-announce/2007/Jul/msg00001.html
* BID: 24873
http://www.securityfocus.com/bid/24873
* FRSIRT: ADV-2007-2510
http://www.frsirt.com/english/advisories/2007/2510
* SECTRACK: 1018373
http://www.securitytracker.com/id?1018373
* SECUNIA: 26034
http://secunia.com/advisories/26034
* XF: quicktime-java-information-disclosure(35361)
http://xforce.iss.net/xforce/xfdb/35361

CVE Reference: CVE-2007-2402

❖ **16564 QuickTime design issue may allow loading arbitrary libraries and freeing arbitrary memory (Remote File Checking)**

A design issue exists in QuickTime for Java. JDirect exposes interfaces that may allow loading arbitrary libraries and freeing arbitrary memory. By enticing a user to visit a web page containing a maliciously crafted Java applet, an attacker can trigger the issue which may lead to arbitrary code execution.

The issue has been fixed in version 7.2.0.

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

References:

* CONFIRM:
http://docs.info.apple.com/article.html?artnum=305947
* APPLE: APPLE-SA-2007-07-11
http://lists.apple.com/archives/Security-announce/2007/Jul/msg00001.html
* BID: 24873
http://www.securityfocus.com/bid/24873
* FRSIRT: ADV-2007-2510
http://www.frsirt.com/english/advisories/2007/2510
* SECTRACK: 1018373
http://www.securitytracker.com/id?1018373

* SECUNIA: 26034
http://secunia.com/advisories/26034
* XF: quicktime-jdirect-code-execution(35360)
http://xforce.iss.net/xforce/xfdb/35360

CVE Reference: CVE-2007-2396

❖ 16563 QuickTime design issue may allow Java applets to bypass security checks in order to read and write process memory (Remote File Checking)

A design issue exists in QuickTime for Java. This may allow Java applets to bypass security checks in order to read and write process memory. By enticing a user to visit a web page containing a maliciously crafted Java applet, an attacker can trigger the issue which may lead to arbitrary code execution.

The issue has been fixed in version 7.2.0.

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

References:

* CONFIRM:
http://docs.info.apple.com/article.html?artnum=305947
* APPLE: APPLE-SA-2007-07-11
http://lists.apple.com/archives/Security-announce/2007/Jul/msg00001.html
* BID: 24873
http://www.securityfocus.com/bid/24873
* FRSIRT: ADV-2007-2510
http://www.frsirt.com/english/advisories/2007/2510
* SECTRACK: 1018373
http://www.securitytracker.com/id?1018373
* SECUNIA: 26034
http://secunia.com/advisories/26034
* XF: quicktime-java-applet-code-execution(35359)
http://xforce.iss.net/xforce/xfdb/35359

CVE Reference: CVE-2007-2393

❖ 16347 BIND query_addsoa Denial of Service Vulnerability

A sequence of queries can cause a recursive nameserver to exit. While it is unlikely these will occur in normal operation, an attack can use them to cause the affected versions to exit. This attack is a denial of service, and does not allow an attacker to gain control of affected systems.

The vulnerability has been fixed in versions BIND 9.4.1 and BIND 9.5.0a4.

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

References:

* CONFIRM:
http://www.isc.org/index.pl?/sw/bind/bind-security.php
* MANDRIVA: MDKSA-2007:100
http://www.mandriva.com/security/advisories?name=MDKSA-2007:100
* CERT-VN: VU#718460
http://www.kb.cert.org/vuls/id/718460
* BID: 23738
http://www.securityfocus.com/bid/23738
* FRSIRT: ADV-2007-1593
http://www.frsirt.com/english/advisories/2007/1593
* SECTRACK: 1017985
http://www.securitytracker.com/id?1017985
* SECUNIA: 25070
http://secunia.com/advisories/25070
* XF: bind-queryaddsoa-dos(33988)
http://xforce.iss.net/xforce/xfdb/33988

CVE Reference: CVE-2007-2241

❖ 16346 BIND allow-query-cache/allow-recursion default acls not set Vulnerability

The default access control lists (acls) are not being correctly set. If not set anyone can make recursive queries and/or query the cache contents.

The vulnerability has been fixed in versions BIND 9.4.2, 9.5.0a6

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

References:

* CONFIRM:
http://www.isc.org/index.pl?/sw/bind/bind-security.php
* MANDRIVA: MDKSA-2007:149
http://www.mandriva.com/security/advisories?name=MDKSA-2007:149
* OPENPKG: OpenPKG-SA-2007.022
http://www.openpkg.com/security/advisories/OpenPKG-SA-2007.022.html
* FRSIRT: ADV-2007-2628
http://www.frsirt.com/english/advisories/2007/2628
* SECTRACK: 1018441
http://www.securitytracker.com/id?1018441
* SECUNIA: 26227
http://secunia.com/advisories/26227
* XF: isc-bind-acl-security-bypass(35571)
http://xforce.iss.net/xforce/xfdb/35571

CVE Reference: CVE-2007-2925

❖ 16562 QuickTime design issue may allow security checks to be disabled (Remote File Checking)

A design issue exists in QuickTime for Java, which may allow security checks to be disabled. By enticing a user to visit a web page containing a maliciously crafted Java applet, an attacker can trigger the issue which may lead to arbitrary code execution.

The issue has been fixed in version 7.2.0.

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

References:

* CONFIRM:
http://docs.info.apple.com/article.html?artnum=305947
* APPLE: APPLE-SA-2007-07-11
http://lists.apple.com/archives/Security-announce/2007/Jul/msg00001.html
* BID: 24873
http://www.securityfocus.com/bid/24873
* FRSIRT: ADV-2007-2510
http://www.frsirt.com/english/advisories/2007/2510
* SECTRACK: 1018373
http://www.securitytracker.com/id?1018373
* SECUNIA: 26034
http://secunia.com/advisories/26034
* XF: quicktime-applet-code-execution(35358)
http://xforce.iss.net/xforce/xfdb/35358

CVE Reference: CVE-2007-2397

❖ 16561 QuickTime integer overflow vulnerability when handling SMIL files (Remote File Checking)

An integer overflow vulnerability exists in QuickTime's handling of SMIL files. By enticing a user to access a maliciously crafted SMIL file, an attacker can trigger the issue which may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.2.0.

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

References:

* IDEFENSE: 20070711 Apple QuickTime SMIL File Processing Integer Overflow Vulnerability
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=556
* BUGTRAQ: 20070717 Re: iDefense Security Advisory 07.11.07: Apple QuickTime SMIL File Processing Integer Overflow Vulnerability
http://www.securityfocus.com/archive/1/archive/1/473882/100/100/threaded
* CONFIRM:
http://docs.info.apple.com/article.html?artnum=305947

* APPLE: APPLE-SA-2007-07-11
http://lists.apple.com/archives/Security-announce/2007/Jul/msg00001.html
* BID: 24873
http://www.securityfocus.com/bid/24873
* FRSIRT: ADV-2007-2510
http://www.frsirt.com/english/advisories/2007/2510
* SECTRACK: 1018373
http://www.securitytracker.com/id?1018373
* SECUNIA: 26034
http://secunia.com/advisories/26034
* XF: quicktime-smil-overflow(35357)
http://xforce.iss.net/xforce/xfdb/35357

CVE Reference: CVE-2007-2394

❖ 16560 QuickTime integer overflow vulnerability when handling .m4v files (Remote File Checking)

An integer overflow vulnerability exists in QuickTime's handling of .m4v files. By enticing a user to access a maliciously crafted .m4v file, an attacker can trigger the issue which may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.2.0.

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

References:

* MISC:
http://security-protocols.com/sp-x46-advisory.php
* CONFIRM:
http://docs.info.apple.com/article.html?artnum=305947
* APPLE: APPLE-SA-2007-07-11
http://lists.apple.com/archives/Security-announce/2007/Jul/msg00001.html
* BID: 23652
http://www.securityfocus.com/bid/23652
* FRSIRT: ADV-2007-2510
http://www.frsirt.com/english/advisories/2007/2510
* OSVDB: 35578
http://www.osvdb.org/35578
* SECTRACK: 1017967
http://www.securitytracker.com/id?1017967
* SECTRACK: 1018373
http://www.securitytracker.com/id?1018373
* SECUNIA: 26034
http://secunia.com/advisories/26034

CVE Reference: CVE-2007-2296

❖ 16559 QuickTime memory corruption issue when handling movie files Vulnerability (Remote File Checking)

A memory corruption issue exists in QuickTime's handling of movie files. By enticing a user to access a maliciously crafted movie file, an attacker can trigger the issue which may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.2.0.

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

References:

* CONFIRM:
http://docs.info.apple.com/article.html?artnum=305947
* APPLE: APPLE-SA-2007-07-11
http://lists.apple.com/archives/Security-announce/2007/Jul/msg00001.html
* CERT-VN: VU#582681
http://www.kb.cert.org/vuls/id/582681
* BID: 24873
http://www.securityfocus.com/bid/24873
* FRSIRT: ADV-2007-2510
http://www.frsirt.com/english/advisories/2007/2510
* SECTRACK: 1018373
http://www.securitytracker.com/id?1018373
* SECUNIA: 26034
http://secunia.com/advisories/26034
* XF: quicktime-moviefile-code-execution(35353)
http://xforce.iss.net/xforce/xfdb/35353

CVE Reference: CVE-2007-2392

❖ 16558 QuickTime memory corruption issue when handling H.264 movies Vulnerability (Remote File Checking)

A memory corruption issue exists in QuickTime's handling of H.264 movies. By enticing a user to access a maliciously crafted H.264 movie, an attacker can trigger the issue which may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.2.0.

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

References:

* MISC:
http://security-protocols.com/sp-x45-advisory.php
* CONFIRM:
http://docs.info.apple.com/article.html?artnum=305947
* APPLE: APPLE-SA-2007-07-11
http://lists.apple.com/archives/Security-announce/2007/Jul/msg00001.html
* BID: 23650
http://www.securityfocus.com/bid/23650
* FRSIRT: ADV-2007-2510
http://www.frsirt.com/english/advisories/2007/2510

* OSVDB: 35577
http://www.osvdb.org/35577
* SECTRACK: 1017965
http://www.securitytracker.com/id?1017965
* SECTRACK: 1018373
http://www.securitytracker.com/id?1018373
* SECUNIA: 26034
http://secunia.com/advisories/26034
* XF: quicktime-h264-code-execution(35356)
http://xforce.iss.net/xforce/xfdb/35356

CVE Reference: CVE-2007-2295

New Vulnerabilities found this Week

Yahoo! Widgets YDP ActiveX Control Buffer Overflow Vulnerability
"Execution of arbitrary code"

Parvez Anwar has discovered a vulnerability in Yahoo! Widgets, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error within the YDPCTL.YDPControl.1 (YDPCTL.dll) ActiveX control when handling the "GetComponentVersion()" method. This can be exploited to cause a stack-based buffer overflow by passing an overly long string (greater than 512 bytes) to the affected method.

Successful exploitation allows execution of arbitrary code.

The vulnerability is confirmed in YDPCTL.dll version 2007.4.13.1 included in Yahoo! Widgets version 4.0.3 (build 178). Other versions may also be affected.

References:
http://help.yahoo.com/l/us/yahoo/widgets/security/security-08.html

Apple iPhone Multiple Vulnerabilities
"Cross-site scripting; Spoofing attacks; Execution of arbitrary code"

Some vulnerabilities have been reported in Apple iPhone, which can be exploited by malicious people to conduct cross-site scripting and spoofing attacks, and potentially to compromise a vulnerable system.

1) A race condition error when updating a page in combination with HTTP redirection may allow Javascript code from one page to modify a redirected page.

2) A boundary error in the Perl Compatible Regular Expressions (PCRE) library used by the Javascript engine in Safari can be exploited to cause a heap-based buffer overflow when a user visits a malicious web page.

Successful exploitation may allow execution of arbitrary code.

3) An HTTP injection issue in XMLHttpRequest can be exploited to inject arbitrary HTTP requests.

4) An error in WebKit within in the handling of International Domain Name (IDN) support and Unicode fonts embedded in Safari can be exploited to spoof a URL by registering domain names with certain international characters that resembles other commonly used characters.

5) An invalid type conversion when rendering frame sets may allow execution of arbitrary code.

References:
http://docs.info.apple.com/article.html?artnum=306173

Mac OS X Security Update Fixes Multiple Vulnerabilities
"Manipulate memory; Code execution"

Apple has issued a security update for Mac OS X, which fixes multiple vulnerabilities.

1) An error within the handling of FTP URIs in CFNetwork can be exploited to run arbitrary FTP commands in context of the user's FTP client, when a user is enticed to click on a specially crafted FTP URI.

2) An input validation error can cause applications using CFNetwork to become vulnerable to HTTP response splitting attacks.

3) A design error exists in the Java interface to CoreAudio, which can be exploited to free arbitrary memory, when a user is enticed to visit a web site containing a specially crafted Java applet.

4) An unspecified error exists in the Java interface to CoreAudio, which can be exploited to read or write out of bounds of the allocated heap by enticing a user to visit a web site containing a specially crafted Java applet.

5) A unspecified error exists in the Java interface to CoreAudio, which can be exploited to instantiate or manipulate objects outside the bounds of the allocated heap, when a user is enticed to visit a web site containing a specially crafted Java applet.

Successful exploitation of vulnerabilities #3 to #5 may allow arbitrary code execution.

6) Two vulnerabilities in cscope can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges and by malicious people to potentially compromise a user's system.

7) A boundary error within the UPnP IGD (Internet Gateway Device Standardized Device Control Protocol) code in iChat can be exploited on the local network to crash the application or to execute arbitrary code, by sending a specially crafted packet.

8) Some vulnerabilities in Kerberos can be exploited by malicious users and malicious people to compromise a vulnerable system.

9) An error within the UPnP IGD (Internet Gateway Device Standardized Device Control Protocol) code in mDNSResponder can be exploited on the local network to crash the application or to execute arbitrary code, by sending a specially crafted packet.

10) An integer underflow exists in PDFKit within the handling of PDF files in Preview and may be exploited to execute arbitrary code when a user opens a specially crafted PDF file.

11) Multiple vulnerabilities exist in PHP, which can be exploited to disclose potentially sensitive information, to cause a DoS (Denial of Service), to bypass certain security restrictions, to conduct cross-site scripting attacks, or to compromise a vulnerable system.

12) An error exists in Quartz Composer due to an uninitialized object pointer when handling Quartz Composer files and may be exploited to execute arbitrary code when a specially crafted Quartz Composer file is viewed.

13) Some vulnerabilities exist in Samba, which can be exploited by malicious people to compromise a vulnerable system.

14) An unspecified error in Samba can be exploited to bypass file system quotas.

15) Some vulnerabilities in Squirrelmail can be exploited by malicious people to disclose and manipulate certain sensitive information or to conduct cross-site scripting, cross-site request forgery, and script insertion attacks.

16) Some vulnerabilities in Apache Tomcat can be exploited by malicious people to conduct cross-site scripting attacks or to bypass certain security restrictions.

17) An error in WebCore can be exploited to load Java applets even when Java is disabled in the preferences.

18) An error in WebCore can be exploited to conduct cross-site scripting attacks.

19) An error in WebCore can be exploited by malicious people to gain knowledge of sensitive information.

20) An error in WebCore when handling properties of certain global objects can be exploited to conduct cross-site scripting attacks when navigating to a new URL with Safari.

21) An error in WebKit within in the handling of International Domain Name (IDN) support and Unicode fonts embedded in Safari can be exploited to spoof a URL.

22) A boundary error in the Perl Compatible Regular Expressions (PCRE) library in WebKit and used by the JavaScript engine in Safari can be exploited to cause a heap-based buffer overflow when a user visits a malicious web page.

23) Input validation errors exists in bzgrep and zgrep.

References:
http://docs.info.apple.com/article.html?artnum=306172

Nessus Vulnerability Scanner ScanCtrl ActiveX Control Insecure Methods
"Overwrite or delete arbitrary files"

Some vulnerabilities have been discovered in Nessus Vulnerability Scanner, which can be exploited by malicious people to overwrite or delete arbitrary files or compromise a

vulnerable system.

The vulnerabilities are caused due to the SCANCTRL.ScanCtrlCtrl.1 (scan.dll) ActiveX control including the insecure "deleteReport()", "deleteNessusRC()", "saveNessusRC()", and "addsetConfig()" methods. These can be exploited to e.g. delete or corrupt arbitrary files on the system or load malicious script code and then save it in an arbitrary location on a user's system in the context of the currently logged-on user.

The vulnerabilities are confirmed on version 3.0.6. Prior versions may also be affected.

References:
http://milw0rm.com/exploits/4230
http://milw0rm.com/exploits/4237

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