netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 14

April 6, 2007

Table of Contents

Product Focus

Sasser Worm Scanner – The Sasser 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 Microsoft SSL Vulnerability (MS04-011) that used by the Sasser Worm to infect machines.

This Week in Review

Take a look at mobile security. Online banking customers want security. Security vs. performance. Hackers selling subscriptions to their services.

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

- **Mobile Device Security Software Forecast**

The mobile worker population is multiplying as mobile devices become thinner and smaller, enabling employees to carry them everywhere they go. Similarly, the opportunity to lose these devices, along with the sensitive corporate information they contain, is also becoming greater. As a result, protecting corporate intellectual property on laptops, mobile phones, and converged mobile devices is at the top of the list for many IT departments, making mobile device security software a hot growth area. According to a new forecast from IDC, worldwide mobile security license and

maintenance revenue exceeds $200 million today and will continue to grow at a healthy compound annual growth rate (CAGR) through the forecast period.

technews

Full Story :
http://www.technologynewsdaily.com/node/6543

❖ Online banking customers value security more than convenience

Nine out of 10 consumers are prepared to sacrifice convenience in favour of stronger security to protect online bank accounts, research has found.
A survey of more than 2,750 consumers found that loss of personal data and the possibility of future financial fraud in their name were the two most frequently cited worries about online banking.

Asked about their preference for convenience versus stronger security, just 10% of respondents said they would sacrifice security for greater convenience.

Computerworlduk

Full Story :
http://www.computerworlduk.com/management/online/e-business/news/index.cfm?RSS&newsid=2484

❖ Network security vs network performance—the line is blurring

Networking and security have always been at odds. On a fundamental level, the goal of the networking group is to rapidly move packets (the good ones) from one host to the next; the security group's job is to stop packets (the bad ones) from getting to the next host and wreaking havoc. And between these two ideals lies an efficient and secure network. Getting to that happy medium is often a challenge.

The networking and security industries reflect this dichotomy with strong security companies and strong networking companies. Sure, the major networking vendors have bought up a slew of security companies in recent years, but we really haven't seen much integration across those products.

Express computer

Full Story :
http://www.expresscomputeronline.com/20070409/technology03.shtml

❖ Hackers Selling Their Dark Services to Highest Bidders

Malware development and distribution has gone commercial, security researchers say.

Webmasters that want to infect visitors to their site with malicious code -- as many phony bank web sites do -- can now buy subscription services from hackers that develop malware. Some of these hacker web sites also offer technical support and pay web site

owners for "clean installs" of their malicious code on end-user systems.

Historically, banks have been major targets of hackers and other IT criminals.

As part of a subscription offered to fraudsters, hackers are selling alert services in which they provide information about upcoming signatures to be released by antivirus vendors.

Banknet360

Full Story :
http://www.banknet360.com/news/NewsAbstract.do;jsessionid=925E7386C1C52A8DD817AE1E30D11BE0?na_id=8298&service_id=1&bi_id=

New Vulnerabilities Tested in SecureScout

- **16464 GDI Local Elevation of Privilege Vulnerability (MS07-017/925902) (Remote File Checking)**

A privilege elevation vulnerability exists in the Graphics Rendering Engine in the way that it starts applications. This vulnerability could allow a logged on user to take complete control of the system.

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

References:

Original advisory:
MS07-017
http://www.microsoft.com/technet/security/Bulletin/MS07-017.mspx

Other references:
MISC: http://projects.info-pull.com/mokb/MOKB-06-11-2006.html
MISC: http://kernelwars.blogspot.com/2007/01/alive.html
MISC: http://www.blackhat.com/html/bh-europe-07/bh-eu-07-speakers.html#Eriksson
BID:20940
URL:http://www.securityfocus.com/bid/20940
FRSIRT:ADV-2006-4358
URL:http://www.frsirt.com/english/advisories/2006/4358
SECTRACK:1017168
URL:http://securitytracker.com/id?1017168
SECUNIA:22668
URL:http://secunia.com/advisories/22668
XF:windows-gdi-kernel-privilege-escalation(30042)
URL:http://xforce.iss.net/xforce/xfdb/30042

CVE Reference: CVE-2006-5758

- **16465 WMF Denial of Service Vulnerability (MS07-017/925902) (Remote File Checking)**

A denial of service vulnerability exists in Windows when rendering Windows Metafile

(WMF) image format files. An attacker who successfully exploited this vulnerability could cause the affected system to stop responding and possibly restart.

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

References:

Original advisory:
MS07-017
http://www.microsoft.com/technet/security/Bulletin/MS07-017.mspx

Other references:
http://xforce.iss.net/xforce/xfdb/33258

CVE Reference: CVE-2007-1211

❖ 16466 EMF Elevation of Privilege Vulnerability (MS07-017/925902) (Remote File Checking)

An elevation of privilege vulnerability exists in the rendering of Enhanced Metafile (EMF) image format files. Any program that renders EMF images on the affected systems could be vulnerable to this attack. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

References:

Original advisory:
MS07-017
http://www.microsoft.com/technet/security/Bulletin/MS07-017.mspx

CVE Reference: CVE-2007-1212

❖ 16467 GDI Invalid Window Size Elevation of Privilege Vulnerability (MS07-017/925902) (Remote File Checking)

A privilege elevation vulnerability exists in the Graphics Rendering Engine in the way that it renders layered application windows. This vulnerability could allow a logged on user to take complete control of the system.

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

References:

Original advisory:
MS07-017
http://www.microsoft.com/technet/security/Bulletin/MS07-017.mspx

CVE Reference: CVE-2006-5586

❖ 16468 Windows Animated Cursor Remote Code Execution Vulnerability (MS07-017/925902) (Remote File Checking)

A remote code execution vulnerability exists in the way that Windows handles cursor, animated cursor, and icon formats. An attacker could try to exploit the vulnerability by constructing a malicious cursor or icon file that could potentially allow remote code execution if a user visited a malicious Web site or viewed a specially crafted e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

References:

Original advisory:
MS07-017
http://www.microsoft.com/technet/security/Bulletin/MS07-017.mspx

Other references:
BUGTRAQ:20070330 0-day ANI vulnerability in Microsoft Windows (CVE-2007-0038)
URL:http://www.securityfocus.com/archive/1/archive/1/464269/100/0/threaded
BUGTRAQ:20070330 Re: 0-day ANI vulnerability in Microsoft Windows (CVE-2007-0038)
URL:http://www.securityfocus.com/archive/1/archive/1/464339/100/0/threaded
BUGTRAQ:20070331 RE: [Full-disclosure] 0-day ANI vulnerability in Microsoft Windows(CVE-2007-0038)
URL:http://www.securityfocus.com/archive/1/archive/1/464342/100/0/threaded
BUGTRAQ:20070331 Re: 0-day ANI vulnerability in Microsoft Windows (CVE-2007-0038)
URL:http://www.securityfocus.com/archive/1/archive/1/464340/100/0/threaded
FULLDISC:20070330 0-day ANI vulnerability in Microsoft Windows (CVE-2007-0038)
URL:http://archives.neohapsis.com/archives/fulldisclosure/2007-03/0470.html
MILW0RM:3634
URL:http://milw0rm.com/exploits/3634
MISC:
http://www.determina.com/security_center/security_advisories/securityadvisory_0day_032907.asp
CERT:TA07-089A
URL:http://www.us-cert.gov/cas/techalerts/TA07-089A.html
CERT-VN:VU#191609
URL:http://www.kb.cert.org/vuls/id/191609
SECUNIA:24659
URL:http://secunia.com/advisories/24659
XF:windows-ani-code-execution(33301)
URL:http://xforce.iss.net/xforce/xfdb/33301

CVE Reference: CVE-2007-0038

❖ 16469 GDI Incorrect Parameter Local Elevation of Privilege Vulnerability

(MS07-017/925902) (Remote File Checking)

A local elevation of privilege vulnerability exists in the Graphics Device Interface due to the way it processes color-related parameters. This vulnerability could allow an attacker to take complete control of the system.

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

References:

Original advisory:
MS07-017
http://www.microsoft.com/technet/security/Bulletin/MS07-017.mspx

CVE Reference: CVE-2007-1215

❖ 16470 Font Rasterizer Vulnerability (MS07-017/925902) (Remote File Checking)

A local elevation of privilege vulnerability exists in the TrueType Fonts rasterizer in the way that it handles defective or modified font types. This vulnerability could allow a logged-on user to take complete control of the system.

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

References:

Original advisory:
MS07-017
http://www.microsoft.com/technet/security/Bulletin/MS07-017.mspx

CVE Reference: CVE-2007-1213

❖ 16471 Wireshark LLT dissector Denial of Service Vulnerability (Remote File Checking)

Unspecified vulnerability in the LLT dissector in Wireshark (formerly Ethereal) 0.99.3 and 0.99.4 allows remote attackers to cause a denial of service (application crash) via unspecified vectors.

The vulnerabilities are reported in various versions prior to 0.99.5.

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

References:

Original Advisory:
http://www.wireshark.org/security/wnpa-sec-2007-01.html

Other references:
CONFIRM: https://issues.rpath.com/browse/RPL-985
FEDORA:FEDORA-2007-207

URL:http://fedoranews.org/cms/node/2565
MANDRIVA:MDKSA-2007:033
URL:http://www.mandriva.com/security/advisories?name=MDKSA-2007:033
REDHAT:RHSA-2007:0066
URL:http://www.redhat.com/support/errata/RHSA-2007-0066.html
BID:22352
URL:http://www.securityfocus.com/bid/22352
FRSIRT:ADV-2007-0443
URL:http://www.frsirt.com/english/advisories/2007/0443
SECTRACK:1017581
URL:http://securitytracker.com/id?1017581
SECUNIA:24016
URL:http://secunia.com/advisories/24016
SECUNIA:24011
URL:http://secunia.com/advisories/24011
SECUNIA:24025
URL:http://secunia.com/advisories/24025
SECUNIA:24084
URL:http://secunia.com/advisories/24084
SECUNIA:24515
URL:http://secunia.com/advisories/24515
XF:wireshark-lltdissector-dos(32056)
URL:http://xforce.iss.net/xforce/xfdb/32056

CVE Reference: CVE-2007-0456

❖ 16472 Wireshark IEEE 802.11 dissector Denial of Service Vulnerability (Remote File Checking)

Unspecified vulnerability in the IEEE 802.11 dissector in Wireshark (formerly Ethereal) 0.10.14 through 0.99.4 allows remote attackers to cause a denial of service (application crash) via unspecified vectors.

The vulnerabilities are reported in various versions prior to 0.99.5.

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

References:

Original Advisory:
http://www.wireshark.org/security/wnpa-sec-2007-01.html

Other references:
CONFIRM: https://issues.rpath.com/browse/RPL-985
FEDORA:FEDORA-2007-207
URL:http://fedoranews.org/cms/node/2565
MANDRIVA:MDKSA-2007:033
URL:http://www.mandriva.com/security/advisories?name=MDKSA-2007:033
REDHAT:RHSA-2007:0066
URL:http://www.redhat.com/support/errata/RHSA-2007-0066.html
BID:22352
URL:http://www.securityfocus.com/bid/22352
FRSIRT:ADV-2007-0443

URL:http://www.frsirt.com/english/advisories/2007/0443
SECTRACK:1017581
URL:http://securitytracker.com/id?1017581
SECUNIA:24016
URL:http://secunia.com/advisories/24016
SECUNIA:24011
URL:http://secunia.com/advisories/24011
SECUNIA:24025
URL:http://secunia.com/advisories/24025
SECUNIA:24084
URL:http://secunia.com/advisories/24084
SECUNIA:24515
URL:http://secunia.com/advisories/24515
XF:wireshark-ieeedissector-dos(32055)
URL:http://xforce.iss.net/xforce/xfdb/32055

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

CVE Reference: CVE-2007-0457

❖ 16473 Wireshark HTTP dissector Denial of Service Vulnerability (Remote File Checking)

Unspecified vulnerability in the HTTP dissector in Wireshark (formerly Ethereal) 0.99.3 and 0.99.4 allows remote attackers to cause a denial of service (application crash) via unspecified vectors, a different issue than CVE-2006-5468.

The vulnerabilities are reported in various versions prior to 0.99.5.

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

References:

Original Advisory:
http://www.wireshark.org/security/wnpa-sec-2007-01.html

Other references:
CONFIRM: https://issues.rpath.com/browse/RPL-985
FEDORA:FEDORA-2007-207
URL:http://fedoranews.org/cms/node/2565
MANDRIVA:MDKSA-2007:033
URL:http://www.mandriva.com/security/advisories?name=MDKSA-2007:033
REDHAT:RHSA-2007:0066
URL:http://www.redhat.com/support/errata/RHSA-2007-0066.html
BID:22352
URL:http://www.securityfocus.com/bid/22352
FRSIRT:ADV-2007-0443
URL:http://www.frsirt.com/english/advisories/2007/0443
SECTRACK:1017581
URL:http://securitytracker.com/id?1017581
SECUNIA:24016
URL:http://secunia.com/advisories/24016

SECUNIA:24011
URL:http://secunia.com/advisories/24011
SECUNIA:24025
URL:http://secunia.com/advisories/24025
SECUNIA:24084
URL:http://secunia.com/advisories/24084
SECUNIA:24515
URL:http://secunia.com/advisories/24515
XF:wireshark-httpdissector-dos(32054)
URL:http://xforce.iss.net/xforce/xfdb/32054

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

CVE Reference: CVE-2007-0458

New Vulnerabilities found this Week

Yahoo! Messenger AudioConf ActiveX Control Buffer Overflow

"Execution of arbitrary code"

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

The vulnerability is caused due to a boundary error within the AudioConf ActiveX control (yacscom.dll) component of Yahoo! Messenger. This can be exploited to cause a stack-based buffer overflow by setting the "socksHostname" and "hostName" properties to an overly large string and then calling the "createAndJoinConference()" method.

Successful exploitation allows execution of arbitrary code when a user visits a malicious web site.

The vulnerability is reported in version 8.x. Other versions may also be affected.

References:
http://messenger.yahoo.com/security_update.php?id=031207
http://www.zerodayinitiative.com/advisories/ZDI-07-012.html

Microsoft Windows Animated Cursor Buffer Overflow Vulnerability

"Execution of arbitrary code"

A vulnerability has been discovered in Microsoft Windows, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error within the handling of animated cursors and can be exploited to cause a stack-based buffer overflow via a specially crafted animated cursor file.

Successful exploitation allows execution of arbitrary code when a user e.g. visits a malicious website using Internet Explorer or opens a malicious e-mail message.

NOTE: The vulnerability is currently being actively exploited.

References:
http://www.microsoft.com/technet/security/Bulletin/MS07-017.mspx
http://descriptions.securescout.com/tc/16468

Microsoft Windows GDI Multiple Vulnerabilities
"Denial of Service; Gain escalated privileges"

Multiple vulnerabilities have been reported in Microsoft Windows, which can be exploited by malicious, local users to gain escalated privileges and by malicious people to cause a DoS (Denial of Service) and potentially compromise a user's system.

1) An error within the handling of GDI kernel structures allows the created global shared memory section, which is mapped with read-only permissions, to be re-mapped with read-write permissions. This can be exploited to corrupt memory by overwriting the data structures with arbitrary data.

2) An error within the processing of Windows Metafile (WMF) image format files can be exploited to cause a system to stop responding or crash when viewing a malicious WMF file.

3) A boundary error within the processing of Enhanced Metafile (EMF) image format files can be exploited to execute arbitrary code on a system via any application rendering EMF files.

4) An error in the Graphics Rendering Engine when rendering layered application windows with invalid window sizes can be exploited to execute arbitrary code with escalated privileges.

5) An error in the Graphics Device Interface when processing color-related parameters can be exploited to execute arbitrary code with escalated privileges.

6) An error in the TrueType Fonts rasterizer when handling defective or modified font types may be exploited to execute arbitrary code via a specially crafted font type.

References:
http://www.microsoft.com/technet/security/Bulletin/MS07-017.mspx
http://descriptions.securescout.com/tc/16464
http://descriptions.securescout.com/tc/16465
http://descriptions.securescout.com/tc/16466
http://descriptions.securescout.com/tc/16467
http://descriptions.securescout.com/tc/16469
http://descriptions.securescout.com/tc/16470

Mozilla Firefox Firebug Extension "console.log()" Cross-Context Scripting
"Execute arbitrary script code"

pdp has reported a vulnerability in the Firebug extension for Mozilla Firefox, which can be exploited by malicious people to compromise a vulnerable system.

Firebug does not properly sanitize input passed to the "console.log()" function. This can be exploited to e.g. execute arbitrary script code within the "chrome:" context by tricking

a user into visiting a malicious website.

The vulnerability is reported in versions prior to 1.02.

References:
https://addons.mozilla.org/en-US/firefox/addons/versions/1843

SAP RFC Library Multiple Vulnerabilities
"Disclose potentially sensitive information; Denial of Service"

Mariano Nuñez Di Croce has reported some vulnerabilities in SAP RFC Library, which can be exploited by malicious people to disclose potentially sensitive information, cause a DoS (Denial of Service), and compromise a vulnerable system.

1) The "RFC_SET_REG_SERVER_PROPERTY" RFC function allows to define the exclusive use of the RFC Server. This can be exploited to cause a DoS by denying access to other clients.

2) An unspecified buffer overflow exists within the "SYSTEM_CREATE_INSTANCE" RFC function, which can be exploited to execute arbitrary code.

3) An unspecified buffer overflow exists within the "RFC_START_GUI" RFC function, which can be exploited to execute arbitrary code.

4) Two unspecified errors exist within the "RFC_START_PROGRAM" RFC function. These can be exploited to gain knowledge about the RFC server's configuration or execute arbitrary code.

5) An error within the "TRUSTED_SYSTEM_SECURITY" function can be exploited to gain knowledge about existing user accounts and groups on a RFC server.

The vulnerabilities are reported in SAP RFC Library versions 6.40 and 7.00. Other versions may also be affected.

References:
http://www.cybsec.com/vuln/CYBSEC-Security_Advisory_SAP_RFC_SET_REG_SERVER_PROPERTY_RFC_Function_Denial_of_Service.pdf
http://www.cybsec.com/vuln/CYBSEC-Security_Advisory_SAP_RFC_START_GUI_RFC_Function_Buffer_Overflow.pdf
http://www.cybsec.com/vuln/CYBSEC-Security_Advisory_SAP_RFC_START_PROGRAM_RFC_Function_Multiple_Vulnerabilities.pdf
http://www.cybsec.com/vuln/CYBSEC-Security_Advisory_SAP_SYSTEM_CREATE_INSTANCE_RFC_Function_Buffer_Overflow.pdf
http://www.cybsec.com/vuln/CYBSEC-Security_Advisory_SAP_TRUSTED_SYSTEM_SECURITY_RFC_Function_Information_Disclosure.pdf

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