netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 8

February 22, 2008

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.

Check out our video section for a number of interviews with Jesper Jurcenoks:
www.netvigilance.com/videos

This Week in Review

Free honeypot for Windows offered by netVigilance.New Microsoft idea under attack. Large hacking network busted in Canada. Easy to hijack magnetic stripe info.

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

- **NetVigilance offers a free Windows honeypot**

Network vulnerability-assessment vendor NetVigilance is offering a'free tool called WinHoneyd as a low-interaction honeypot that can mimic aspects of a Windows-based network to be used as an attack decoy.
The intent of the WinHoneyd honeypot, says NetVigilance CEO Jesper Jurcenoks, is to emulate the real corporate network, either at the Internet edge or deep inside the LAN, by means of a honeypot so the impact of attacks can be better understood.

"As soon as you have a guy probing your fake server, you can use this information to create better countermeasures," said Jurcenoks. "The honeypot can be a way to learn about new attacks."

Pc-welt

Full Story :
http://www.pcwelt.de/index.cfm?pid=829&pk=61812

❖ Security guru scoffs at Microsoft worm idea

Security super-guru Bruce Schneier has ridiculed Microsoft's controversial idea that software could be patched using 'worm-like' programs.
Last week, researchers at Microsoft's UK lab in Cambridge said they planned to present the idea of using patching that mimicked the 'self-replicating' behaviour of computer worms to the IEEE's Infocom conference in April.

According to Microsoft, the advantage of such a design would be speed and resilience. In an age of zero-day attacks, such an idea could offer benefits.

techworld

Full Story :
http://www.techworld.com/security/news/index.cfm?newsID=11498&pagtype=samechan

❖ International hacking network busted, Quebec police say

Computers in Manitoba, the United States, Poland and Brazil targeted in scam
Quebec provincial police say they've dismantled a computer hacking network that targeted unprotected personal computers around the world.

Police raided several homes across Quebec on Wednesday and arrested 16 people in their investigation, which they say uncovered the largest hacking scam in Canadian history.

The hackers collaborated online to attack and take control of as many as one million computers around the world that were not equipped with anti-virus software or firewalls, said provincial police captain Frederick Gaudreau.

Cbc news

Full Story :
http://www.cbc.ca/technology/story/2008/02/20/qc-hackers0220.html

- **Researcher Hacks into Credit Card Magnetic Strips**

RFID security guru releases a test program that can read chip and PIN credit cards using the EMV standard.

WASHINGTON – Personally identifiable information baked into the magnetic strip on your credit card can be easily hijacked by hackers using lightweight tools, according to a warning from RFID security guru Adam Laurie.

At the Black Hat DC briefings here, Laurie announced the release of CHaP.py, a test program created to read chip and PIN credit cards using the EMV standard.

EMV, named for the three companies that developed the standard – Europay, MasterCard and VISA – handles authentication of credit and debit card payments.

eweek

Full Story :
http://www.eweek.com/c/a/Security/Researcher-Hacks-Into-Credit-Card-Magnetic-Strips/

New Vulnerabilities Tested in SecureScout

- **16725 Oracle Application Server - OC4J component unspecified Vulnerability (jul-2006/AS04)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server OC4J component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/440758/100/100/threaded
* CERT: TA06-200A
http://www.us-cert.gov/cas/techalerts/TA06-200A.html
* BID: 19054

http://www.securityfocus.com/bid/19054
* FRSIRT: ADV-2006-2863
http://www.frsirt.com/english/advisories/2006/2863
* FRSIRT: ADV-2006-2947
http://www.frsirt.com/english/advisories/2006/2947
* SECTRACK: 1016529
http://securitytracker.com/id?1016529
* SECUNIA: 21111
http://secunia.com/advisories/21111
* SECUNIA: 21165
http://secunia.com/advisories/21165
* XF: oracle-cpu-july-2006(27897)
http://xforce.iss.net/xforce/xfdb/27897

CVE Reference: CVE-2006-3709

❖ 16726 Oracle Application Server - OC4J component unspecified Vulnerability (jul-2006/AS05)

An unspecified vulnerability with unknown impact exists in Oracle Application Server OC4J component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/440758/100/100/threaded
* CERT: TA06-200A
http://www.us-cert.gov/cas/techalerts/TA06-200A.html
* BID: 19054
http://www.securityfocus.com/bid/19054
* FRSIRT: ADV-2006-2863
http://www.frsirt.com/english/advisories/2006/2863
* FRSIRT: ADV-2006-2947
http://www.frsirt.com/english/advisories/2006/2947
* SECTRACK: 1016529
http://securitytracker.com/id?1016529
* SECUNIA: 21111
http://secunia.com/advisories/21111
* SECUNIA: 21165
http://secunia.com/advisories/21165
* XF: oracle-cpu-july-2006(27897)
http://xforce.iss.net/xforce/xfdb/27897

CVE Reference: CVE-2006-3710

❖ 16727 Oracle Application Server - OC4J component unspecified Vulnerability (jul-2006/AS06)

An unspecified vulnerability with unknown impact exists in Oracle Application Server OC4J component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/440758/100/100/threaded
* CERT: TA06-200A
http://www.us-cert.gov/cas/techalerts/TA06-200A.html
* BID: 19054
http://www.securityfocus.com/bid/19054
* FRSIRT: ADV-2006-2863
http://www.frsirt.com/english/advisories/2006/2863
* FRSIRT: ADV-2006-2947
http://www.frsirt.com/english/advisories/2006/2947
* SECTRACK: 1016529
http://securitytracker.com/id?1016529
* SECUNIA: 21111
http://secunia.com/advisories/21111
* SECUNIA: 21165
http://secunia.com/advisories/21165
* XF: oracle-cpu-july-2006(27897)
http://xforce.iss.net/xforce/xfdb/27897

CVE Reference: CVE-2006-3711

❖ 16860 Active Directory Vulnerability (MS08-003/946538) (Remote File Checking)

A denial of service vulnerability exists in implementations of Active Directory on Microsoft Windows 2000 and Windows Server 2003. The vulnerability also exists in

implementations of Active Directory Application Mode (ADAM) when installed on Windows XP and Windows Server 2003. The vulnerability is due to improper validation of specially crafted LDAP requests. An attacker who successfully exploited this vulnerability could cause the computer to stop responding and automatically restart.

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

References:

* MS: MS08-003
http://www.microsoft.com/technet/security/bulletin/ms08-003.mspx
* CERT: TA08-043C
http://www.us-cert.gov/cas/techalerts/TA08-043C.html
* BID: 27638
http://www.securityfocus.com/bid/27638
* FRSIRT: ADV-2008-0505
http://www.frsirt.com/english/advisories/2008/0505/references
* SECTRACK: 1019382
http://www.securitytracker.com/id?1019382
* SECUNIA: 28764
http://secunia.com/advisories/28764

CVE Reference: CVE-2008-0088

❖ 16861 Windows Vista TCP/IP Vulnerability (MS08-004/946456) (Remote File Checking)

A denial of service vulnerability exists in TCP/IP processing in Windows Vista. An attacker could exploit the vulnerability by creating a specially crafted DHCP server that returns a specially crafted packet to a host, corrupting TCP/IP structures and causing the affected system to stop responding and automatically restart.

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

References:

* MS: MS08-004
http://www.microsoft.com/technet/security/bulletin/ms08-004.mspx
* CERT: TA08-043C
http://www.us-cert.gov/cas/techalerts/TA08-043C.html
* BID: 27634
http://www.securityfocus.com/bid/27634
* FRSIRT: ADV-2008-0506
http://www.frsirt.com/english/advisories/2008/0506/references
* SECTRACK: 1019383
http://www.securitytracker.com/id?1019383
* SECUNIA: 28828
http://secunia.com/advisories/28828

CVE Reference: CVE-2008-0084

❖ 16862 File Change Notification Vulnerability (MS08-005/942831) (Remote File Checking)

A local elevation of privilege vulnerability exists in the way that the Internet Information Service handles file change notifications in the FTPRoot, NNTPFile\Root, and WWWRoot folders. An attacker who successfully exploited this vulnerability could execute arbitrary code in the context of local system. An attacker could then install programs; view, change, or delete data; or create new accounts with full administrative rights.

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

References:

* MS: MS08-005
http://www.microsoft.com/technet/security/bulletin/ms08-005.mspx
* CERT: TA08-043C
http://www.us-cert.gov/cas/techalerts/TA08-043C.html
* BID: 27101
http://www.securityfocus.com/bid/27101
* FRSIRT: ADV-2008-0507
http://www.frsirt.com/english/advisories/2008/0507/references
* SECTRACK: 1019384
http://www.securitytracker.com/id?1019384
* SECUNIA: 28849
http://secunia.com/advisories/28849

CVE Reference: CVE-2008-0074

❖ 16863 ASP Vulnerability (MS08-006/942830) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Information Services handles input to ASP Web pages. An attacker could exploit the vulnerability by passing malicious input to a Web site's ASP page. An attacker who successfully exploited this vulnerability could then perform any actions on the IIS Server with the same rights as the Worker Process Identity (WPI), which by default is configured with Network Service account privileges.

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

References:

* MS: MS08-006
http://www.microsoft.com/technet/security/bulletin/ms08-006.mspx
* CERT: TA08-043C
http://www.us-cert.gov/cas/techalerts/TA08-043C.html

* BID: 27676
http://www.securityfocus.com/bid/27676
* FRSIRT: ADV-2008-0508
http://www.frsirt.com/english/advisories/2008/0508/references
* SECTRACK: 1019385
http://www.securitytracker.com/id?1019385
* SECUNIA: 28893
http://secunia.com/advisories/28893

CVE Reference: CVE-2008-0075

❖ 16864 Microsoft Works File Converter Input Validation Vulnerability (MS08-011/947081) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Works File Converter due to the way that it improperly validates section length headers with the .wps format. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts.

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

References:

* IDEFENSE: 20080208 Microsoft Office Works Converter Heap Overflow Vulnerability
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=659
* MS: MS08-011
http://www.microsoft.com/technet/security/bulletin/ms08-011.mspx
* CERT: TA08-043C
http://www.us-cert.gov/cas/techalerts/TA08-043C.html
* BID: 27657
http://www.securityfocus.com/bid/27657
* FRSIRT: ADV-2008-0513
http://www.frsirt.com/english/advisories/2008/0513/references
* SECTRACK: 1019386
http://www.securitytracker.com/id?1019386
* SECUNIA: 28904
http://secunia.com/advisories/28904

CVE Reference: CVE-2007-0216

❖ 16865 Microsoft Works File Converter Index Table Vulnerability (MS08-011/947081) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Works File Converter due to the way that it improperly validates section header index table information with the .wps file format. An attacker who successfully exploited this vulnerability could take

complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts.

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

References:

* MS: MS08-011
http://www.microsoft.com/technet/security/bulletin/ms08-011.mspx
* CERT: TA08-043C
http://www.us-cert.gov/cas/techalerts/TA08-043C.html
* BID: 27658
http://www.securityfocus.com/bid/27658
* FRSIRT: ADV-2008-0513
http://www.frsirt.com/english/advisories/2008/0513/references
* SECTRACK: 1019387
http://www.securitytracker.com/id?1019387
* SECUNIA: 28904
http://secunia.com/advisories/28904

CVE Reference: CVE-2008-0105

❖ 16866 Microsoft Works File Converter Field Length Vulnerability (MS08-011/947081) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Works File Converter due to the way that it improperly validates various field lengths information with the .wps file format. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts.

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

References:

* IDEFENSE: 20080208 Microsoft Office Works Converter Stack-based Buffer Overflow Vulnerability
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=660
* MS: MS08-011
http://www.microsoft.com/technet/security/bulletin/ms08-011.mspx
* CERT: TA08-043C
http://www.us-cert.gov/cas/techalerts/TA08-043C.html
* BID: 27659
http://www.securityfocus.com/bid/27659
* FRSIRT: ADV-2008-0513
http://www.frsirt.com/english/advisories/2008/0513/references
* SECTRACK: 1019388
http://www.securitytracker.com/id?1019388
* SECUNIA: 28904

http://secunia.com/advisories/28904

CVE Reference: CVE-2008-0108

New Vulnerabilities found this Week

Opera Multiple Vulnerabilities

"Cross-site scripting attacks; disclose sensitive information"

Some vulnerabilities have been reported in Opera, which can be exploited by malicious people to conduct cross-site scripting attacks, disclose sensitive information, or to bypass certain security restrictions.

1) A security issue is caused due to a design error when handling input to file form fields, which can potentially be exploited to trick a user into uploading arbitrary files.

2) An error within the handling of custom comments in image properties can be exploited to execute arbitrary script code in the wrong security context when comments of a malicious image are displayed.

3) An error in the handling of attribute values when importing XML into a document can be exploited to bypass filters and conduct cross-site scripting attacks if these values are used as document content.

The vulnerabilities are reported in versions prior to 9.26.

References:
http://www.opera.com/support/search/view/877/
http://www.opera.com/support/search/view/879/
http://www.opera.com/support/search/view/880/

BEA WebLogic Products Multiple Vulnerabilities

"Script insertion; Session fixation; Cross-site scripting; Brute force attacks; Disclose sensitive information"

Some vulnerabilities, security issues, and a weakness have been reported in various BEA WebLogic products, which can be exploited by malicious users to conduct script insertion attacks, and by malicious people to conduct session fixation, cross-site scripting, or brute force attacks, disclose sensitive information, or to bypass certain security restrictions.

References:
http://dev2dev.bea.com/pub/advisory/256
http://dev2dev.bea.com/pub/advisory/257
http://dev2dev.bea.com/pub/advisory/258
http://dev2dev.bea.com/pub/advisory/261
http://dev2dev.bea.com/pub/advisory/262

http://dev2dev.bea.com/pub/advisory/263
http://dev2dev.bea.com/pub/advisory/264
http://dev2dev.bea.com/pub/advisory/265
http://dev2dev.bea.com/pub/advisory/266
http://dev2dev.bea.com/pub/advisory/267
http://dev2dev.bea.com/pub/advisory/268
http://dev2dev.bea.com/pub/advisory/269
http://dev2dev.bea.com/pub/advisory/270
http://dev2dev.bea.com/pub/advisory/271
http://dev2dev.bea.com/pub/advisory/273
http://dev2dev.bea.com/pub/advisory/274
http://dev2dev.bea.com/pub/advisory/275

Netscape Multiple Vulnerabilities

"Disclose sensitive information; Conduct spoofing attacks"

Netscape has acknowledged some weaknesses, a security issue, and some vulnerabilities in Netscape Navigator, which can be exploited by malicious people to disclose sensitive information, bypass certain security restrictions, conduct spoofing attacks, or to compromise a user's system.

References:
http://browser.netscape.com/releasenotes/

Linux Kernel Multiple Vulnerabilities

"Denial of Service; Gain escalated privileges"

Some vulnerabilities have been reported in the Linux Kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service) and potentially gain escalated privileges.

References:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.24.2

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