

Table of Contents

[Product Focus](#)

[This Week in Review](#)

[Top Security News Stories this Week](#)

[New Vulnerabilities Tested in SecureScout](#)

[New Vulnerabilities found this Week](#)

Product Focus

[Spida Digispid Worm Scanner](#) – The Spida Digispid Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are prone any of the Microsoft Java Virtual Machine Vulnerabilities (MS02-069).

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.

SANS version 7 (November 2006) support has been added to the SecureScout products.

This Week in Review

Support for new security standard not strong enough yet. A majority of online users want stronger security. Maybe new cryptography with quantum mechanics will end web hacking. Keep watching out for ‘Storm Worm’ infected emails.

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

- ❖ Credit card industry struggling with security standard

Major credit card companies have made it mandatory for merchants and payment processors to comply with stringent network security rules that went into effect in mid-2005. But getting buy-in from the millions of companies that handle credit card information remains elusive.

American Express, Visa International, MasterCard Worldwide and Discover Financial Services are among the backers of the rules known as the Payment Card Industry Data Security Standard (PCI DSS).

"All the merchants are required to comply with the PCI data-security standards or face fines," says Rob Tourt, vice president of network services at Discover. Yet adoption of PCI DSS is not widespread, Tourt admits, though he wouldn't disclose exact figures.

To improve compliance, Discover is getting more aggressive and working individually with certain merchants to make sure they get through the 12-point security plan, which covers firewalls, vulnerability assessment and encryption, among other requirements.

Discover isn't alone in striving to turn PCI DSS into more than a paper tiger. Visa, which works more directly with acquiring banks than with merchants, also is trying to shore up low merchant adoption numbers.

Visa's new approach calls for levying punitive fines on banks that fail to get their merchant customers to comply with the PCI standard -- while promising multimillion-dollar incentive packages for banks that prod their largest customers into complying.

ComputerWorld

Full Story :

<http://www.computerworld.com.sg/ShowPage.aspx?pagetype=2&articleid=4507&pubid=3&tab=Home&issueid=102>

❖ Users call for tougher security for online banking

... methods.

The survey questioned 1,678 adults from eight countries about their opinions on fraud threats such as phishing and keylogging, and on the efforts of their financial institutions to strengthen remote banking authentication.

The results showed that 91% of account-holders are willing to start using a new authentication method, beyond the standard username-and-password format, if their banks decided to offer stronger security.

In addition, 73% said they would like their financial institution to use risk-based authentication, and 69% of account-holders believe that financial institutions should replace username-and-password log-ins with stronger authentication for online banking.

Also, 58% of account-holders believed that financial institutions should deploy stronger

authentication for telephone banking, and 82% wanted their banks to monitor online banking sessions and telephone banking sessions for signs of irregular activity or behaviour - similar to the way that credit card transactions are monitored today.

ComputerWeekly

Full Story :

<http://www.computerweekly.com/Articles/2007/01/26/221424/users-call-for-tougher-security-for-online-banking.htm>

❖ **Quantum cryptography could stop Web hackers**

A Calgary scientist is working on a security technology that could one day make Internet hacking a concern of the past.

Dr. Wolfgang Tittel from the University of Calgary's Centre for Information Security and Cryptography is working with a team to develop secure encryption technology using quantum mechanics.

Most of today's data sent over the Internet is sent electronically. Tittel is using fibre optics to send data on light photons that can move so fast, they can teleport themselves from one place to another instantly.

The researchers are using quantum mechanics to create a new level of cryptography that will be able to tell a user whether personal information is accessed.

"What it allows us is to send a 'quantum key' in a way that we can see, after sending it, whether it has been corrupted, meaning that somebody else has information about this key," Tittel explained on Canada AM.

A hacker can't copy a quantum key without changing it. That's because the security codes are carried in bundles with a particular configuration. If these bundles are disrupted during transmission, they re-configure and the information scrambles.

Ctv news

Full Story :

http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20070126/quantum_codes_070126/20070126?hub=SciTech

❖ **'Storm Worm' Continues to Spread Around Globe**

Virus writers are taking advantage of the winter storms ravaging Northern Europe to launch a malware blitz of their own.

Experts are forecasting an increase in spam as a result of the "Storm" worm that sent out six separate waves containing hundreds of thousands of e-mails this past weekend, and continues to touch down on computers worldwide.

"The malware is distributed to set up a network of infected zombie computers, which can then be used to launch massive spam campaigns," said Commtouch Chief Technology Officer Amir Lev, in a statement.

The Small.Dam worm, dubbed "Storm" because of its reference to a major storm in Europe in its subject line, was first uncovered during the week of Jan. 15. With tabloid-style subject lines such as "230 dead as storm batters Europe" and "First nuclear act of terrorism!", the worm has spread internationally since it was first discovered.

The e-mails contained attachments with names like "full clip.exe" and "read more.exe", an example of social engineering common among malware writers. Once a user opens the attachment, the Trojan creates a backdoor that the malware writers can exploit in the future.

FOXNews

Full Story :

<http://www.foxnews.com/story/0,2933,247098,00.html?sPage=fnc.technology/cybersecurity>

New Vulnerabilities Tested in SecureScout

❖ 13519 Oracle Database Server - Export component Buffer Overflow Vulnerability (jan-2007/DB11)

A Buffer Overflow vulnerability exists in Oracle Database Server Export component.

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

References:

Original Advisory:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html>

Other references:

http://www.red-database-security.com/advisory/oracle_cpu_jan_2007.html

Product Homepage:

<http://www.oracle.com/>

CVE Reference: [CVE-2007-0277](#)

❖ 13520 Oracle Database Server - NLS Runtime component Buffer Overflow Vulnerability (jan-2007/DB12)

A Buffer Overflow vulnerability exists in Oracle Database Server NLS Runtime component.

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

References:

Original Advisory:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html>

Other references:

http://www.red-database-security.com/advisory/oracle_cpu_jan_2007.html

Product Homepage:

<http://www.oracle.com/>

CVE Reference: [CVE-2007-0278](#)

❖ **13521 Oracle Database Server - Oracle Net Services component Buffer Overflow Vulnerability (jan-2007/DB13)**

A Buffer Overflow vulnerability exists in Oracle Database Server Oracle Net Services component.

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

References:

Original Advisory:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html>

Other references:

http://www.red-database-security.com/advisory/oracle_cpu_jan_2007.html

Product Homepage:

<http://www.oracle.com/>

CVE Reference: [CVE-2007-0276](#)

❖ **13522 Oracle Database Server - Oracle Text component Buffer Overflow Vulnerability (jan-2007/DB14)**

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/cpujan2007.html>

Other references:

http://www.red-database-security.com/advisory/oracle_cpu_jan_2007.html

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

CVE Reference: [CVE-2007-0278](#)

❖ **13523 A Buffer Overflow vulnerability exists in Oracle Database Server Oracle Text component.**

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/cpujan2007.html>

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_jan_2007.html

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

CVE Reference: [CVE-2007-0268](#)

❖ **13524 Oracle Database Server - Recovery Manager component Buffer Overflow Vulnerability (jan-2007/DB16)**

A Buffer Overflow vulnerability exists in Oracle Database Server Recovery Manager component.

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

References:

Original Advisory:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html>

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_jan_2007.html

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

CVE Reference: [CVE-2007-0276](#)

❖ **16398 Wireshark SCSI dissector Denial of Service Vulnerability (Remote**

File Checking)

Unspecified vulnerability in the SCSI dissector in Wireshark (formerly Ethereal) 0.99.2 allows remote attackers to cause a denial of service (crash) via unspecified vectors.

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

References:

Original Advisory:

<http://www.wireshark.org/security/wnpa-sec-2006-02.html>

Other references:

CONFIRM: <http://support.avaya.com/elmodocs2/security/ASA-2006-227.htm>
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>
REDHAT:RHSA-2006:0658
URL:<http://www.redhat.com/support/errata/RHSA-2006-0658.html>
CERT-VN:VU#808832
URL:<http://www.kb.cert.org/vuls/id/808832>
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>
SECUNIA:21885
URL:<http://secunia.com/advisories/21885>
SECUNIA:22378
URL:<http://secunia.com/advisories/22378>
XF:wireshark-scsi-dos(28550)
URL:<http://xforce.iss.net/xforce/xfdb/28550>
XF:wireshark-esp-offbyone(28553)
URL:<http://xforce.iss.net/xforce/xfdb/28553>

Product Homepage:

<http://www.wireshark.org/>

CVE Reference: [CVE-2006-4330](https://cve.org/CVE-2006-4330)

❖ **16399 Wireshark IPSec ESP preference parser Off-by-one errors Vulnerability (Remote File Checking)**

Multiple off-by-one errors in the IPsec ESP preference parser in Wireshark (formerly Ethernet) 0.99.2 allow remote attackers to cause a denial of service (crash) via unspecified vectors.

The vulnerabilities have been reported in version 0.99.2.

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

References:

Original Advisory:

<http://www.wireshark.org/security/wnpa-sec-2006-02.html>

Other references:

CONFIRM: <http://support.avaya.com/elmodocs2/security/ASA-2006-227.htm>
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>
REDHAT:RHSA-2006:0658
URL:<http://www.redhat.com/support/errata/RHSA-2006-0658.html>
CERT-VN:VU#638376
URL:<http://www.kb.cert.org/vuls/id/638376>
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>
SECUNIA:21885
URL:<http://secunia.com/advisories/21885>
SECUNIA:22378
URL:<http://secunia.com/advisories/22378>
XF:wireshark-esp-offbyone(28553)
URL:<http://xforce.iss.net/xforce/xfdb/28553>

Product Homepage:

<http://www.wireshark.org/>

CVE Reference: [CVE-2006-4331](#)

❖ 16400 Wireshark DHCP dissector Denial of Service Vulnerability (Remote File Checking)

Unspecified vulnerability in the DHCP dissector in Wireshark (formerly Ethernet) 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.wireshark.org/security/wnpa-sec-2006-02.html>

Other references:

GENTOO:GLSA-200608-26

[URL:http://security.gentoo.org/glsa/glsa-200608-26.xml](http://security.gentoo.org/glsa/glsa-200608-26.xml)

MANDRIVA:MDKSA-2006:152

[URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:152](http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:152)

CERT-VN:VU#335656

[URL:http://www.kb.cert.org/vuls/id/335656](http://www.kb.cert.org/vuls/id/335656)

BID:19690

[URL:http://www.securityfocus.com/bid/19690](http://www.securityfocus.com/bid/19690)

FRSIRT:ADV-2006-3370

[URL:http://www.frsirt.com/english/advisories/2006/3370](http://www.frsirt.com/english/advisories/2006/3370)

SECTrack:1016736

[URL:http://securitytracker.com/id?1016736](http://securitytracker.com/id?1016736)

SECUNIA:21597

[URL:http://secunia.com/advisories/21597](http://secunia.com/advisories/21597)

SECUNIA:21649

[URL:http://secunia.com/advisories/21649](http://secunia.com/advisories/21649)

SECUNIA:21619

[URL:http://secunia.com/advisories/21619](http://secunia.com/advisories/21619)

SECUNIA:21682

[URL:http://secunia.com/advisories/21682](http://secunia.com/advisories/21682)

XF:wireshark-dhcp-dos(28554)

[URL:http://xforce.iss.net/xforce/xfdb/28554](http://xforce.iss.net/xforce/xfdb/28554)

XF:wireshark-esp-offbyone(28553)

[URL:http://xforce.iss.net/xforce/xfdb/28553](http://xforce.iss.net/xforce/xfdb/28553)

Product Homepage:

<http://www.wireshark.org/>

CVE Reference: [CVE-2006-4332](#)

❖ **16401 Wireshark SSCOP dissector Denial of Service Vulnerability (Remote File Checking)**

The SSCOP dissector in Wireshark (formerly Ethereal) before 0.99.3 allows remote attackers to cause a denial of service (resource consumption) via malformed packets that cause the Q.2391 dissector to use excessive memory.

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.wireshark.org/security/wnpa-sec-2006-02.html>

Other references:

CONFIRM: <http://support.avaya.com/elmodocs2/security/ASA-2006-227.htm>
DEBIAN:DSA-1171
[URL:http://www.debian.org/security/2006/dsa-1171](http://www.debian.org/security/2006/dsa-1171)
GENTOO:GLSA-200608-26
[URL:http://security.gentoo.org/glsa/glsa-200608-26.xml](http://security.gentoo.org/glsa/glsa-200608-26.xml)
MANDRIVA:MDKSA-2006:152
[URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:152](http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:152)
REDHAT:RHSA-2006:0658
[URL:http://www.redhat.com/support/errata/RHSA-2006-0658.html](http://www.redhat.com/support/errata/RHSA-2006-0658.html)
CERT-VN:VU#696896
[URL:http://www.kb.cert.org/vuls/id/696896](http://www.kb.cert.org/vuls/id/696896)
BID:19690
[URL:http://www.securityfocus.com/bid/19690](http://www.securityfocus.com/bid/19690)
FRSIRT:ADV-2006-3370
[URL:http://www.frsirt.com/english/advisories/2006/3370](http://www.frsirt.com/english/advisories/2006/3370)
SECTrack:1016736
[URL:http://securitytracker.com/id?1016736](http://securitytracker.com/id?1016736)
SECUNIA:21597
[URL:http://secunia.com/advisories/21597](http://secunia.com/advisories/21597)
SECUNIA:21649
[URL:http://secunia.com/advisories/21649](http://secunia.com/advisories/21649)
SECUNIA:21813
[URL:http://secunia.com/advisories/21813](http://secunia.com/advisories/21813)
SECUNIA:21619
[URL:http://secunia.com/advisories/21619](http://secunia.com/advisories/21619)
SECUNIA:21682
[URL:http://secunia.com/advisories/21682](http://secunia.com/advisories/21682)
SECUNIA:21885
[URL:http://secunia.com/advisories/21885](http://secunia.com/advisories/21885)
SECUNIA:22378
[URL:http://secunia.com/advisories/22378](http://secunia.com/advisories/22378)
XF:wireshark-sscop-dos(28556)
[URL:http://xforce.iss.net/xforce/xfdb/28556](http://xforce.iss.net/xforce/xfdb/28556)
XF:wireshark-esp-offbyone(28553)
[URL:http://xforce.iss.net/xforce/xfdb/28553](http://xforce.iss.net/xforce/xfdb/28553)

Product Homepage:

<http://www.wireshark.org/>

CVE Reference: [CVE-2006-4333](#)

New Vulnerabilities found this Week

Adobe Reader Unspecified Heap Corruption Vulnerability
“Execution of arbitrary code”

Piotr Bania has reported a vulnerability in Adobe Reader, which can potentially be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an unspecified error when processing PDF files. This can be exploited to cause a heap corruption and may allow execution of arbitrary code when a specially-crafted PDF file is opened.

The vulnerability is reported in version 7.0.8 and prior. Other versions may also be affected.

References:

<http://www.piotrbania.com/all/adv/adobe-acrobat-adv.txt>
<http://www.adobe.com/support/security/bulletins/apsb07-01.html>
<http://www.kb.cert.org/vuls/id/698924>

Citrix Presentation Server Print Provider Buffer Overflow Vulnerability

“Execution of arbitrary code”

A vulnerability has been reported in Citrix Presentation Server, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in a print provider (ccprov.dll) when handling arguments passed to the "EnumPrintersW()" and "OpenPrinter()" functions. This can be exploited to e.g. cause a stack-based buffer overflow by passing an overly long string (more than 130 bytes) as the first argument to the "OpenPrinter()" function through a local API call or RPC request.

Successful exploitation allows execution of arbitrary code.

The vulnerability reportedly affects Citrix MetaFrame XP and Presentation Server version 4.0 and prior.

References:

<http://support.citrix.com/article/CTX111686>
<http://www.zerodayinitiative.com/advisories/ZDI-07-006.html>

ISC BIND Unspecified Denial of Service Vulnerability

“Denial of Service”

A vulnerability has been reported in ISC BIND, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an unspecified error, which may cause the named daemon to dereference a freed fetch context.

Successful exploitation crashes the named daemon.

NOTE: A potential security issue related to the validation of type ANY responses has also been reported.

References:

<http://www.isc.org/index.pl?sw/bind/view/?release=9.2.8>
<http://www.isc.org/index.pl?sw/bind/view/?release=9.3.4>

<http://marc.theaimsgroup.com/?l=bind-announce&m=116968519321296&w=2>

Symantec Web Security Two Vulnerabilities

“Denial of Service”

Two vulnerabilities have been reported in Symantec Web Security, which can be exploited by malicious people to conduct cross-site scripting attacks or to cause a DoS (Denial of Service).

- 1) An error when handling large files can be exploited to cause the system to slow down by using the license registering interface to submit a very large file.
- 2) Input passed to certain parameters in unspecified files is not properly sanitized before being returned to the user when displaying certain pages. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

The vulnerabilities are reported in versions prior to 3.0.1.85.

References:

<http://securityresponse.symantec.com/avcenter/security/Content/2007.01.24c.html>

Apple Mac OS X QuickDraw Denial of Service

“Denial of Service”

LMH has reported a vulnerability in Apple Mac OS X, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in Apple QuickDraw and can be exploited to cause the application using the QuickDraw routines to crash, when a specially crafted PICT image is processed.

The vulnerability is reported in Mac OS X 10.4.8 (x86). Other versions may also be affected.

References:

<http://projects.info-pull.com/moab/MOAB-23-01-2007.html>

Apple Mac OS X "UserNotificationCenter" Privilege Escalation

“Gain escalated privileges”

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

The vulnerability is caused due to UserNotificationCenter.app running any InputManager within /Library/InputManagers in a user's home directory with privileges of the "wheel" group. This can be exploited to perform certain actions with "wheel" privileges (e.g. replacing "/Applications/System Preferences.app/Contents/Resources/installAssistant").

NOTE: If diskutil is invoked by an administrator to repair permissions of a volume, the setuid bit is set on "installAssistant", which is owned by the user root.

The vulnerability is reported in Mac OS X 10.4.8 (x86). Other versions may also be affected.

References:

<http://projects.info-pull.com/moab/MOAB-22-01-2007.html>

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