netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 18

May 2, 2008

Table of Contents

Product Focus

Much anticipated "Negev" released.

Our Web-interface for the Perimeter Service is now running dynamic pages based on "Ajax", giving a much improved response time and customer experience. Existing customers can log right into the new system from the usual login page.

Sapphire Worm Scanner – The Sapphire 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 SQL buffer overflow vulnerability (MS02-039/MS02-061) that the recent Sapphire Worm uses to propagate.

CTO Jesper Jurcenoks of netVigilance is the keynote speaker at the ITEC Conference & Exhibition 2008 in Houston May 8, see
http://www.netvigilance.com/events

This Week in Review

debate about securing web 2.0. PCI report says small merchants the culprit. And the hackers are after them. How to protect your data in these modern times.

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

- **Event describes importance of securing Web 2.0**

The Secure Enterprise 2.0 Forum debuted today in New York. The event looked at the advantages and security risks of Web 2.0 technology use in the enterprise, and was sponsored by Credit Suisse and software vendor WorkLight.

While the tone of much of the discussion advocated for the integration of Web 2.0 technology into the corporate environment, highlighting the efficiencies that Web 2.0 applications bring to the work experience, speakers certainly did not neglect the inherent security risks.

scmagazine

Full Story :
http://www.scmagazineus.com/Event-describes-importance-of-securing-Web-20/article/109537/

- **Report: small merchants, not major retailers, biggest threat to credit card fraud**

Credit card thieves are taking advantage of small, brick-and-mortar retailers and of the vulnerabilities in their point-of-sale check-out systems, according to a report by Trustwave, a Payment Card Industry Data Security Standard (PCI DSS) assessor.

The quarterly report belies the popular perceptions that using credit cards online is riskier than using them at a physical store and that large merchants' huge wealth of data make them primary targets for credit card fraud. Rather, it points a finger at traditional small merchants, such as storefronts and fast food outlets.

scmagazine

Full Story :
http://www.scmagazineus.com/Report-small-merchants-not-major-retailers-biggest-threat-to-credit-card-fraud/article/109595/

- **Small Business Means Big Business for Hackers**

Some simple, low-cost solutions also include: maintaining software and hardware to include upgrades, spyware and anti-virus software. Also, make sure the traveling laptop has sufficient security protection in case it gets lost, and don't share or give out any passwords to anyone. Never assume you're safe.
Think your company is too small to attract a hacker? Think again.

"Small businesses are a hacker's dream ... Hackers know that most small business owners have the 'It won't happen to me' or 'I don't have anything that they'd want' mentality and prey on it," said Renee Chronister, co-owner of Parameter Security, an ethical hacking firm.

Sci-tech today

Full Story :
http://www.sci-tech-today.com/story.xhtml?story_id=0010003OSXTL

- **Live Mesh: IT's universal remote**

Apple's .Mac comes close, but Microsoft's Live Mesh may have the remote desktop formula business needs
pple's .Mac comes close to offering professionals secure shared data and remote desktop access without the hassle of VPN. Microsoft Live Mesh hopes to take it all the way.

Old-schoolers will tell you that there are only two places your important data should live: on your meticulously secured network behind a paranoid firewall, or at Iron Mountain. One must heed the old schoolers, for they shall keep the bitemarks off your backside, but their advice must be tempered with modern reality. Having data live exclusively within your domain presents thorny operational problems when two or more people need to get at it. If you want to selectively share files with temporary staff, business partners, external software testers, or employees who are on the road, you've got to find a way to publish it with a combination of easy access and tight security.

computerworld

Full Story :
http://www.computerworld.com.au/index.php/id;1920420944;fp;16;fpid;1

New Vulnerabilities Tested in SecureScout

- **12154 OpenSSH X11 Forwarding Information Disclosure Vulnerability**

A vulnerability has been discovered in OpenSSH, which can be exploited by malicious, local users to disclose sensitive information.

The vulnerability is caused due to sshd improperly binding TCP ports on the local IPV6 interface if required ports on the IPV4 interface are in use. This can be exploited by a malicious, local user to intercept an X11 forwarding session by listening to a port used by sshd to forward the local X11 display (e.g. port 6010/TCP).

The vulnerability is reported in versions 4.3p2 and confirmed in 4.7p1. Other versions

prior to 5.0 may also be affected.

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

Some References:

* BUGTRAQ: 20080325 rPSA-2008-0120-1 gnome-ssh-askpass openssh openssh-client openssh-server
http://www.securityfocus.com/archive/1/archive/1/490054/100/0/threaded
* MLIST: [security-announce] 20080403 Globus Security Advisory 2008-01: GSI-OpenSSH vulnerability
http://www.globus.org/mail_archive/security-announce/2008/04/msg00000.html
* CONFIRM:
http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=463011
* CONFIRM:
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0120
* CONFIRM:
https://issues.rpath.com/browse/RPL-2397
* CONFIRM:
http://sourceforge.net/project/shownotes.php?release_id=590180&group_id=69227
* FREEBSD: FreeBSD-SA-08:05
http://security.FreeBSD.org/advisories/FreeBSD-SA-08:05.openssh.asc
* GENTOO: GLSA-200804-03
http://www.gentoo.org/security/en/glsa/glsa-200804-03.xml
* MANDRIVA: MDVSA-2008:078
http://www.mandriva.com/security/advisories?name=MDVSA-2008:078
* SLACKWARE: SSA:2008-095-01
http://www.slackware.org/security/viewer.php?l=slackware-security&y=2008&m=slackware-security.540188
* SUSE: SUSE-SR:2008:009
http://lists.opensuse.org/opensuse-security-announce/2008-04/msg00007.html
* UBUNTU: USN-597-1
http://www.ubuntulinux.org/support/documentation/usn/usn-597-1
* BID: 28444
http://www.securityfocus.com/bid/28444
* FRSIRT: ADV-2008-0994
http://www.frsirt.com/english/advisories/2008/0994/references
* FRSIRT: ADV-2008-1124
http://www.frsirt.com/english/advisories/2008/1124/references
* FRSIRT: ADV-2008-1123
http://www.frsirt.com/english/advisories/2008/1123/references
* SECTRACK: 1019707
http://www.securitytracker.com/id?1019707
* SECUNIA: 29522
http://secunia.com/advisories/29522
* SECUNIA: 29537
http://secunia.com/advisories/29537
* SECUNIA: 29554
http://secunia.com/advisories/29554
* SECUNIA: 29626
http://secunia.com/advisories/29626
* SECUNIA: 29676
http://secunia.com/advisories/29676
* SECUNIA: 29683

http://secunia.com/advisories/29683
* SECUNIA: 29686
http://secunia.com/advisories/29686
* SECUNIA: 29735
http://secunia.com/advisories/29735
* SECUNIA: 29721
http://secunia.com/advisories/29721
* XF: openssh-sshd-session-hijacking(41438)
http://xforce.iss.net/xforce/xfdb/41438

CVE Reference: CVE-2008-1483

❖ 12155 OpenSSH ForceCommand Bypass Weakness

A weakness has been reported in OpenSSH, which can be exploited by malicious, local users to bypass certain security restrictions.

The weakness is caused due to the improper implementation of the "ForceCommand" directive. This can be exploited to execute arbitrary commands via the ~/.ssh/rc file even if a "ForceCommand" directive is in effect.

The weakness is reported in versions prior to 4.9 and 4.9p1.

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

References:

* BUGTRAQ: 20080404 rPSA-2008-0139-1 gnome-ssh-askpass openssh openssh-client openssh-server
http://www.securityfocus.com/archive/1/archive/1/490488/100/0/threaded
* CONFIRM:
http://www.openssh.com/txt/release-4.9
* CONFIRM:
https://issues.rpath.com/browse/RPL-2419
* CONFIRM:
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0139
* GENTOO: GLSA-200804-03
http://www.gentoo.org/security/en/glsa/glsa-200804-03.xml
* OPENBSD: [4.3] 001: SECURITY FIX: March 30, 2008
http://www.openbsd.org/errata43.html#001_openssh
* SUSE: SUSE-SR:2008:009
http://lists.opensuse.org/opensuse-security-announce/2008-04/msg00007.html
* BID: 28531
http://www.securityfocus.com/bid/28531
* FRSIRT: ADV-2008-1035
http://www.frsirt.com/english/advisories/2008/1035/references
* SECTRACK: 1019733
http://www.securitytracker.com/id?1019733
* SECUNIA: 29602
http://secunia.com/advisories/29602
* SECUNIA: 29609

http://secunia.com/advisories/29609
* SECUNIA: 29683
http://secunia.com/advisories/29683
* SECUNIA: 29693
http://secunia.com/advisories/29693
* SECUNIA: 29735
http://secunia.com/advisories/29735
* XF: openssh-forcecommand-command-execution(41549)
http://xforce.iss.net/xforce/xfdb/41549

CVE Reference: CVE-2008-1657

❖ **16752 Oracle Application Server - Oracle Workflow Cartridge component unspecified Vulnerability (jan-2006/WF02)**

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

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
* CERT-VN: VU#545804
http://www.kb.cert.org/vuls/id/545804
* BID: 16287
http://www.securityfocus.com/bid/16287
* FRSIRT: ADV-2006-0243
http://www.frsirt.com/english/advisories/2006/0243
* FRSIRT: ADV-2006-0323
http://www.frsirt.com/english/advisories/2006/0323
* SECTRACK: 1015499
http://securitytracker.com/id?1015499
* SECUNIA: 18493
http://secunia.com/advisories/18493
* SECUNIA: 18608
http://secunia.com/advisories/18608
* XF: oracle-january2006-update(24321)
http://xforce.iss.net/xforce/xfdb/24321

CVE Reference: CVE-2006-0291

❖ **16753 Oracle Application Server - Oracle Workflow Cartridge component unspecified Vulnerability (jan-2006/WF03)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server

Oracle Workflow Cartridge component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
* CERT-VN: VU#545804
http://www.kb.cert.org/vuls/id/545804
* BID: 16287
http://www.securityfocus.com/bid/16287
* FRSIRT: ADV-2006-0243
http://www.frsirt.com/english/advisories/2006/0243
* FRSIRT: ADV-2006-0323
http://www.frsirt.com/english/advisories/2006/0323
* SECTRACK: 1015499
http://securitytracker.com/id?1015499
* SECUNIA: 18493
http://secunia.com/advisories/18493
* SECUNIA: 18608
http://secunia.com/advisories/18608
* XF: oracle-january2006-update(24321)
http://xforce.iss.net/xforce/xfdb/24321

CVE Reference: CVE-2006-0291

❖ 16754 Oracle Application Server - Protocol Support component unspecified Vulnerability (jan-2006/DBC01)

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

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
* CERT-VN: VU#545804
http://www.kb.cert.org/vuls/id/545804
* BID: 16287
http://www.securityfocus.com/bid/16287
* FRSIRT: ADV-2006-0243
http://www.frsirt.com/english/advisories/2006/0243
* FRSIRT: ADV-2006-0323
http://www.frsirt.com/english/advisories/2006/0323
* SECTRACK: 1015499
http://securitytracker.com/id?1015499
* SECUNIA: 18493
http://secunia.com/advisories/18493

* SECUNIA: 18608
http://secunia.com/advisories/18608
* XF: oracle-january2006-update(24321)
http://xforce.iss.net/xforce/xfdb/24321

CVE Reference: CVE-2006-0282

❖ 16755 Oracle Application Server - Reorganize Objects & Convert Tablespace component unspecified Vulnerability (jan-2006/DBC02)

An unspecified vulnerability with unknown impact exists in Oracle Application Server Reorganize Objects & Convert Tablespace component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
* CERT-VN: VU#545804
http://www.kb.cert.org/vuls/id/545804
* BID: 16287
http://www.securityfocus.com/bid/16287
* FRSIRT: ADV-2006-0243
http://www.frsirt.com/english/advisories/2006/0243
* FRSIRT: ADV-2006-0323
http://www.frsirt.com/english/advisories/2006/0323
* SECTRACK: 1015499
http://securitytracker.com/id?1015499
* SECUNIA: 18493
http://secunia.com/advisories/18493
* SECUNIA: 18608
http://secunia.com/advisories/18608
* XF: oracle-january2006-update(24321)
http://xforce.iss.net/xforce/xfdb/24321

CVE Reference: CVE-2006-0283

❖ 16756 Oracle Application Server - OC4J component unspecified Vulnerability (oct-2005/AS01)

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/pdf/cpuoct2005.html
* CERT: TA05-292A

http://www.us-cert.gov/cas/techalerts/TA05-292A.html
* CERT-VN: VU#210524
http://www.kb.cert.org/vuls/id/210524
* BID: 15134
http://www.securityfocus.com/bid/15134
* SECUNIA: 17250
http://secunia.com/advisories/17250

CVE Reference: CVE-2008-0087

❖ 16916 Wireshark malformed X.509sat or Roofnet packet Denial of Service Vulnerability (Remote File Checking)

The X.509sat or Roofnet dissectors in Wireshark (formerly Ethereal) 0.99.5 through 0.99.8 allows remote attackers to cause a denial of service (crash) via a malformed packet.

The vulnerability has been reported in versions 0.99.5 through 0.99.8.

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

References:

* BUGTRAQ: 20080404 rPSA-2008-0138-1 tshark wireshark
http://www.securityfocus.com/archive/1/archive/1/490487/100/0/threaded
* CONFIRM:
http://www.wireshark.org/security/wnpa-sec-2008-02.html
* CONFIRM:
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0138
* CONFIRM:
https://issues.rpath.com/browse/RPL-2418
* FEDORA: FEDORA-2008-2941
https://www.redhat.com/archives/fedora-package-announce/2008-April/msg00140.html
* FEDORA: FEDORA-2008-3040
https://www.redhat.com/archives/fedora-package-announce/2008-April/msg00228.html
* SUSE: SUSE-SR:2008:008
http://lists.opensuse.org/opensuse-security-announce/2008-04/msg00005.html
* BID: 28485
http://www.securityfocus.com/bid/28485
* FRSIRT: ADV-2008-1007
http://www.frsirt.com/english/advisories/2008/1007/references
* SECTRACK: 1019728
http://www.securitytracker.com/id?1019728
* SECUNIA: 29569
http://secunia.com/advisories/29569
* SECUNIA: 29736
http://secunia.com/advisories/29736
* SECUNIA: 29622
http://secunia.com/advisories/29622
* SECUNIA: 29695
http://secunia.com/advisories/29695
* XF: wireshark-roofnet-dissector-dos(41515)

http://xforce.iss.net/xforce/xfdb/41515
* XF: wireshark-x509sat-dissector-dos(41514)
http://xforce.iss.net/xforce/xfdb/41514

CVE Reference: CVE-2008-1561

❖ 16917 Wireshark malformed LDAP packet Denial of Service Vulnerability (Remote File Checking)

The LDAP dissector in Wireshark (formerly Ethereal) 0.99.2 through 0.99.8 allows remote attackers to cause a denial of service (crash) via a malformed packet.

The vulnerability has been reported in versions 0.99.2 through 0.99.8.

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

References:

* BUGTRAQ: 20080404 rPSA-2008-0138-1 tshark wireshark
http://www.securityfocus.com/archive/1/archive/1/490487/100/0/threaded
* CONFIRM:
http://www.wireshark.org/security/wnpa-sec-2008-02.html
* CONFIRM:
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0138
* CONFIRM:
https://issues.rpath.com/browse/RPL-2418
* FEDORA: FEDORA-2008-2941
https://www.redhat.com/archives/fedora-package-announce/2008-April/msg00140.html
* FEDORA: FEDORA-2008-3040
https://www.redhat.com/archives/fedora-package-announce/2008-April/msg00228.html
* SUSE: SUSE-SR:2008:008
http://lists.opensuse.org/opensuse-security-announce/2008-04/msg00005.html
* BID: 28485
http://www.securityfocus.com/bid/28485
* FRSIRT: ADV-2008-1007
http://www.frsirt.com/english/advisories/2008/1007/references
* SECTRACK: 1019728
http://www.securitytracker.com/id?1019728
* SECUNIA: 29569
http://secunia.com/advisories/29569
* SECUNIA: 29736
http://secunia.com/advisories/29736
* SECUNIA: 29622
http://secunia.com/advisories/29622
* SECUNIA: 29695
http://secunia.com/advisories/29695
* XF: wireshark-ldap-dissector-dos(41516)
http://xforce.iss.net/xforce/xfdb/41516

CVE Reference: CVE-2008-1562

❖ **16918 Wireshark malformed SCCP packet Denial of Service Vulnerability (Remote File Checking)**

The SCCP dissector in Wireshark (formerly Ethereal) 0.99.6 through 0.99.8 allows remote attackers to cause a denial of service (crash) via a malformed packet.

The vulnerability has been reported in versions 0.99.6 through 0.99.8.

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

References:

* BUGTRAQ: 20080404 rPSA-2008-0138-1 tshark wireshark
http://www.securityfocus.com/archive/1/archive/1/490487/100/0/threaded
* CONFIRM:
http://www.wireshark.org/security/wnpa-sec-2008-02.html
* CONFIRM:
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0138
* CONFIRM:
https://issues.rpath.com/browse/RPL-2418
* FEDORA: FEDORA-2008-2941
https://www.redhat.com/archives/fedora-package-announce/2008-April/msg00140.html
* FEDORA: FEDORA-2008-3040
https://www.redhat.com/archives/fedora-package-announce/2008-April/msg00228.html
* SUSE: SUSE-SR:2008:008
http://lists.opensuse.org/opensuse-security-announce/2008-04/msg00005.html
* BID: 28485
http://www.securityfocus.com/bid/28485
* FRSIRT: ADV-2008-1007
http://www.frsirt.com/english/advisories/2008/1007/references
* SECTRACK: 1019728
http://www.securitytracker.com/id?1019728
* SECUNIA: 29569
http://secunia.com/advisories/29569
* SECUNIA: 29736
http://secunia.com/advisories/29736
* SECUNIA: 29622
http://secunia.com/advisories/29622
* SECUNIA: 29695
http://secunia.com/advisories/29695
* XF: wireshark-sccp-dissector-dos(41517)
http://xforce.iss.net/xforce/xfdb/41517

CVE Reference: CVE-2008-1563

New Vulnerabilities found this Week

IBM Lotus Expeditor Client for Desktop "cai" URI Handler Code Execution

“Execute arbitrary programs”

Thomas Pollet has reported a vulnerability in IBM Lotus Expeditor, which can be exploited by malicious people to compromise a user's system.

The problem is that the application registers the "cai" URI handler, which allows launching rcplauncher.exe with arbitrary command line arguments. This can be exploited to execute arbitrary programs via the "-launcher" argument.

The vulnerability affects Lotus Expeditor Client for Desktop version 6.1 on Windows systems using Internet Explorer.

References:
http://www-1.ibm.com/support/docview.wss?uid=swg21303813

WordPress PHP Code Execution and Cross-Site Scripting

“cross-site scripting attacks; bypass the authentication mechanism; gain administrative access; execute arbitrary PHP code”

Two vulnerabilities have been reported in WordPress, which can be exploited by malicious people to conduct cross-site scripting attacks, bypass certain security restrictions, and to compromise a vulnerable system.

1) A vulnerability is caused due to improper access restriction of the administration section. This can be exploited to bypass the authentication mechanism and gain administrative access by setting a specially crafted cookie. This can further be exploited to execute arbitrary PHP code.

Successful exploitation of this vulnerability requires that registering new accounts is enabled.

The vulnerability is reported in version 2.5.

2) Input passed to an unspecified parameter is not properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

The vulnerability is reported in version 2.5. Prior versions may also be affected.

References:
http://wordpress.org/development/2008/04/wordpress-251/

KDE KHTML PNG Processing Buffer Overflow Vulnerability

“Execution of arbitrary code”

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

The vulnerability is caused due to a boundary error in KHTML when processing PNG files. This can be exploited to cause a heap-based buffer overflow via a specially crafted PNG file included in e.g. a malicious web page.

Successful exploitation may allow execution of arbitrary code.

The vulnerability is reported in KHTML included in KDE versions 4.0 through 4.0.3.

References:
http://www.kde.org/info/security/advisory-20080426-1.txt

PhpGedView Unspecified Vulnerability

"Execute arbitrary code"

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

The vulnerability is caused due to an unspecified error, which can be exploited to execute arbitrary code by sending a specially crafted request.

The vulnerability is reported in all versions prior to 4.1.5.

Reference:
http://sourceforge.net/project/shownotes.php?group_id=55456&release_id=595222

Sun Java System Directory Server "bind-dn" Security Bypass

"Gain administrative access"

Sun has acknowledged a vulnerability in Sun Java System Directory Server, which can be exploited by malicious people to bypass certain security restrictions.

The vulnerability is caused due to an unspecified error when classifying connections based on "bind-dn", which can be exploited gain administrative access.

The vulnerability is reported in Sun Java System Directory Server 6.0, 6.1, 6.2, Enterprise Edition for all platforms (Solaris 8, 9, and 10 SPARC and x86 Platforms, Linux, Windows, and HP-UX).

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-66-235381-1

Trillian Display Name Processing Memory Corruption

"Execution of arbitrary code"

Juan Pablo Lopez Yacubian has discovered a vulnerability in Trillian, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an error within the processing of "Display Names" in messages. This can be exploited to cause a memory corruption by e.g. setting the "Display Name" to a specially crafted, overly long string and sending an overly long message to another user using the MSN protocol.

Successful exploitation may allow execution of arbitrary code but requires that the attacker is in the contact list of the target user.

The vulnerability is confirmed in version 3.1.9.0 Basic. Other versions may also be affected.

References:
http://archives.neohapsis.com/archives/bugtraq/2008-04/0315.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