netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 30

July 28, 2006

Table of Contents

Product Focus

HTTP Tunnel – Professional Firewall Piercing with Windows based HTTP Tunnel from netVigilance, get your traffic thru any firewall, supports both incoming and outgoing traffic. Easy GUI configuration Price $25, **download free trial today.**

This Week in Review

MS to push IE 7.0 via autoupdate, SOX getting urgent for NON-US business, Karma Sutra Virus destructive, Mozilla Security Fixes andMike Miller from SecurityProNews details a new “legal” Internet Scam that most of us could fall for.

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

- **Microsoft tags IE 7 'high priority' update**

Microsoft plans to automatically push Internet Explorer 7 to Windows XP users when the browser update is ready later this year.

IE 7 will be delivered in the fourth quarter as a "high priority" update via Automatic Updates in Windows XP, Gary Schare, Microsoft's director of IE product management, said in an interview Tuesday. Automatic Updates is a Windows feature typically used for

security updates, but Microsoft has also used it to push its antipiracy tool WGA Notifications.

"The justification, of course, is the significant security enhancements in IE 7," Schare said. Microsoft recommends that all Windows users install the new browser when it ships, he added.

IE 7 will be the first major update to Microsoft's ubiquitous Web browser in five years. Security was the No. 1 investment for the update, Microsoft has said. Critics have likened predecessor IE 6 to "Swiss cheese" because of the many security vulnerabilities in it. A third and final beta of IE 7 was released late last month.
ZDNet

Full Story :
http://news.zdnet.com/2100-1009_22-6098500.html

❖ SOX clock ticking for overseas businesses

The clock is ticking for non-U.S. companies that need to be compliant with one of the most talked-about elements of the Sarbanes-Oxley Act.

July 15 was the critical milestone for foreign companies listed in the U.S. to be compliant with Section 404 of the act. They now have anything from a few weeks to nearly a year to meet the regulations or face the consequences.

U.S. lawmakers passed the Sarbanes-Oxley Act, also known as SOX, in 2002. The regulations within aim to prevent financial malpractice and accounting scandals like that at Enron. Under Section 404, publicly traded companies must have internal policies and controls in place to protect, document and process information for financial reporting.

The law requires affected businesses to comply by the end of their fiscal year after July 15, 2006. The date is an extension of the original deadline of July 15, 2005, set by the U.S. Securities and Exchange Commission. Public U.S. companies were required to be compliant in November 2004.
ZDNet

Full Story :
http://news.zdnet.com/2100-1009_22-6098931.html

❖ New Kama Sutra worms corrupts Microsoft documents

A new worm that already accounts for one in every 15 pieces of malicious code carries a "nuclear option" payload that corrupts data in a slew of popular file formats, a security company warned Friday.

The Nyxem.e worm, said Finnish security firm F-Secure, carries code that instructs it to replace data in files with .doc, .xls, .mdb, .mde, .ppt, .pps, .zip, .rar, .pdf, .psd, or .dmp extensions with the useless string "DATA Error [47 0F 94 93 F4 K5]" on the third of the month.

Full Story :
http://www.itnews.com.au/newsstory.aspx?CIaNID=23708

- **Mozilla Fires Off Security Update for Firefox Browser**

Mozilla on July 26 started firing out notices to Firefox users recommending they install a newly released version of the browser, v1.5.0.5, which includes some essential security fixes.

ADVERTISEMENT The Mountain View, Calif., company began sending out notices in the early afternoon, notifying users via popup windows.

Chris Beard, vice president of products at Mozilla, told eWEEK that the updated version was released as part of Mozilla's regularly scheduled security and stability update program.

"This release proactively addresses a range of security, performance and stability issues within the Firefox browser," Beard said.

eWeek.com

Full Story :
http://www.eweek.com/article2/0,1895,1994837,00.asp

- **The Biggest Internet Scam In Recent History**

Are you interested in hearing about the biggest internet scam in recent history...

NO! Would you be interested if you discovered that it is possibly you that was scammed several months ago and did not even know it? In fact, if you were scammed back then you probably have had money removed from your bank account every month AND you may not even know you are losing your money. Now you are interested!

This foundation for this breech of internet security started a couple of years ago as a gift from your caring politicians and bureaucrats in the form of bank funds electronic transfer legislation. Simply stated, if you owe anyone money they (whoever) can 'electronically' withdraw it from your account without your permission if they have a contract in place.

A few weeks back a neighbor lady came to me venting her disapproval because some unknown and unnamed internet company had cleaned out her banking account. She was going to complain, bring legal suit and if she could find a real person she was going to do really mean things. It took 5 minutes and three questions to find out she was into a legal binding electronic contract she knew nothing about.
SecurityProNews

Full Story :
http://www.securitypronews.com/news/securitynews/spn-45-20060726TheBiggestInternetScamInRecentHistory.html

New Vulnerabilities Tested in SecureScout

- **12130 PostgreSQL errors in the cryptographic library**

PostgreSQL Database server is a very popular database server which sees widespread use throughout the world.

Signedness errors in the cryptographic library may increase the probability that certain password hashes are generated using the same salt.

PostgreSQL 8.0.x before 8.0.6 and 8.1.x before 8.1.2, are vulnerable to this issue.

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

References:

BUGTRAQ:20060207 crypt_blowfish 1.0
URL:http://www.securityfocus.com/archive/1/archive/1/424260/100/0/threaded
MISC:
http://cvsweb.openwall.com/cgi/cvsweb.cgi/Owl/packages/glibc/crypt_blowfish/crypt_gensalt.c?only_with_tag=CRYPT_BLOWFISH_1_0
REDHAT:RHSA-2006:0526
URL:http://www.redhat.com/support/errata/RHSA-2006-0526.html
SGI:20060602-01-U
URL:ftp://patches.sgi.com/support/free/security/advisories/20060602-01-U.asc
FRSIRT:ADV-2006-0477
URL:http://www.frsirt.com/english/advisories/2006/0477
OSVDB:23005
URL:http://www.osvdb.org/23005
SECUNIA:18772
URL:http://secunia.com/advisories/18772
SECUNIA:20232
URL:http://secunia.com/advisories/20232
SECUNIA:20782
URL:http://secunia.com/advisories/20782
XF:cryptblowfish-salt-information-disclosure(24590)
URL:http://xforce.iss.net/xforce/xfdb/24590

Home page:
http://www.postgresql.org/

CVE Reference: CVE-2006-0591

❖ 13378 Oracle Database Server - OCI component unspecified vulnerability (jul-2006/DB09)

An unspecified vulnerability in the OCI component may allow a remote attacker to compromise system integrity and availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-

updates/cpujul2006.html

Other references:
MISC: http://www.red-database-security.com/exploits/oracle-sql-injection-oracle-dbms_export_extension.html
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
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
CERT-VN:VU#932124
URL:http://www.kb.cert.org/vuls/id/932124
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

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

CVE Reference: CVE-2006-3702

❖ 13379 Oracle Database Server - OCI component unspecified vulnerability (jul-2006/DB10)

An unspecified vulnerability in the OCI component may allow a remote attacker to compromise system integrity and availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
MISC: ttp://www.red-database-security.com/exploits/oracle-sql-injection-oracle-dbms_export_extension.html
CONFIRM: ttp://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
MISC: http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
CERT-VN:VU#932124
URL:http://www.kb.cert.org/vuls/id/932124
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863

URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

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

CVE Reference: CVE-2006-3702

❖ 13380 Oracle Database Server - OCI component unspecified vulnerability (jul-2006/DB11)

An unspecified vulnerability in the OCI component may allow a remote attacker to compromise system integrity and availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
MISC: http://www.red-database-security.com/exploits/oracle-sql-injection-oracle-dbms_export_extension.html
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
CERT:TA06-200A
URL: http://www.us-cert.gov/cas/techalerts/TA06-200A.html
CERT-VN:VU#932124
URL:http://www.kb.cert.org/vuls/id/932124
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

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

CVE Reference: CVE-2006-3702

❖ 13381 Oracle Database Server - OCI component unspecified vulnerability (jul-2006/DB12)

An unspecified vulnerability in the OCI component may allow a remote attacker to compromise system integrity and availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
MISC: http://www.red-database-security.com/exploits/oracle-sql-injection-oracle-dbms_export_extension.html
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
CERT:TA06-200A
URL: http://www.us-cert.gov/cas/techalerts/TA06-200A.html
CERT-VN:VU#932124
URL:http://www.kb.cert.org/vuls/id/932124
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

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

CVE Reference: CVE-2006-3702

❖ 13382 Oracle Database Server - OCI component unspecified vulnerability (jul-2006/DB13)

An unspecified vulnerability in the OCI component may allow a remote attacker to compromise system integrity and availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
MISC: http://www.red-database-security.com/exploits/oracle-sql-injection-oracle-dbms_export_extension.html
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
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
CERT-VN:VU#932124
URL:http://www.kb.cert.org/vuls/id/932124
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

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

CVE Reference: CVE-2006-3702

❖ 13383 Oracle Database Server - OCI component unspecified vulnerability (jul-2006/DB14)

An unspecified vulnerability in the OCI component may allow a remote attacker to compromise system integrity and availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
MISC: http://www.red-database-security.com/exploits/oracle-sql-injection-oracle-dbms_export_extension.html
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
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
CERT-VN:VU#932124
URL:http://www.kb.cert.org/vuls/id/932124
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863

SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

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

CVE Reference: CVE-2006-3702

❖ 13384 Oracle Database Server - Oracle ODBC Driver component unspecified vulnerability (jul-2006/DB15)

An unspecified vulnerability in the Oracle ODBC Driver component may allow a remote attacker to compromise system integrity and availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other 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
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

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

CVE Reference: CVE-2006-3704

❖ 13385 Oracle Database Server - Query Rewrite/Summary Mgmt component unspecified vulnerability (jul-2006/DB16)

An unspecified vulnerability in the Query Rewrite/Summary Mgmt component may allow a remote attacker to compromise system integrity and availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
MISC: http://www.red-database-security.com/exploits/oracle-sql-injection-oracle-dbms_export_extension.html
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
CERT:TA06-200A
URL: http://www.us-cert.gov/cas/techalerts/TA06-200A.html
CERT-VN:VU#932124
URL:http://www.kb.cert.org/vuls/id/932124
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

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

CVE Reference: CVE-2006-3702

❖ 13386 Oracle Database Server - RPC component unspecified vulnerability (jul-2006/DB17)

An unspecified vulnerability in the RPC component may allow a remote attacker to compromise system integrity and availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Other references:
MISC: http://www.red-database-security.com/exploits/oracle-sql-injection-oracle-dbms_export_extension.html
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
CERT:TA06-200A
URL:http://www.us-cert.gov/cas/techalerts/TA06-200A.html
CERT-VN:VU#932124

URL:http://www.kb.cert.org/vuls/id/932124
BID:19054
URL:http://www.securityfocus.com/bid/19054
FRSIRT:ADV-2006-2863
URL:http://www.frsirt.com/english/advisories/2006/2863
SECTRACK:1016529
URL:http://securitytracker.com/id?1016529
SECUNIA:21111
URL:http://secunia.com/advisories/21111

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

CVE Reference: CVE-2006-3702

New Vulnerabilities found this Week

Mozilla Firefox Multiple Vulnerabilities

"Execution of arbitrary code"

Multiple vulnerabilities have been reported in Mozilla Firefox, which can be exploited by malicious people to conduct cross-site scripting attacks or compromise a user's system.

1) An error within the handling of JavaScript references to frames and windows may in certain circumstances result in the reference not being properly cleared and allows execution of arbitrary code.

The vulnerability only affects the 1.5 branch.

2) An error within the handling of Java references to properties of the window.navigator object allows execution of arbitrary code if a web page replaces the navigator object before starting Java.

The vulnerability only affects the 1.5 branch.

3) A memory corruption error within the handling of simultaneously happening XPCOM events results in the use of a deleted timer object and allows execution of arbitrary code.

The vulnerability only affects the 1.5 branch.

4) Insufficient access checks on standard DOM methods of the top-level document object (e.g. "document.getElementById()") can be exploited by a malicious web site to execute arbitrary script code in the context of another site.

The vulnerability only affects the 1.5 branch.

5) A race condition where JavaScript garbage collection deletes a temporary variable still being used in the creation of a new Function object may allow execution of arbitrary code.

The vulnerability only affects the 1.5 branch.

6) Various errors in the JavaScript engine during garbage collection where used pointers are deleted and integer overflows when handling long strings e.g. passed to the

"toSource()" methods of the Object, Array, and String objects may allow execution of arbitrary code.

7) Named JavaScript functions have a parent object created using the standard "Object()" constructor, which can be redefined by script. This can be exploited to run script code with elevated privileges if the "Object()" constructor returns a reference to a privileged object.

8) An error within the handling of PAC script can be exploited by a malicious Proxy AutoConfig (PAC) server to execute script code with escalated privileges by setting the FindProxyForURL function to the eval method on a privileged object that has leaked into the PAC sandbox.

9) An error within the handling of scripts granted the "UniversalBrowserRead" privilege can be exploited to execute script code with escalated privileges equivalent to "UniversalXPConnect".

10) An error can be exploited to execute arbitary script code in context of another site by using the "XPCNativeWrapper(window).Function(...)" construct, which creates a function that appears to belong to another site.

The vulnerability only affects the 1.5 branch.

11) A memory corruption error when calling "nsListControlFrame::FireMenuItemActiveEvent()", some potential string class buffer overflows, a memory corruption error when anonymous box selectors are outside of UA stylesheets, references to removed nodes, errors involving table row and column groups, and an error in "crypto.generateCRMFRequest" callback may potentially be exploited to execute arbitrary code.

12) An error within the handling of "chrome:" URI's can be exploited to reference remote files that can run scripts with full privileges.

References:
http://www.mozilla.org/security/announce/2006/mfsa2006-44.html
http://www.mozilla.org/security/announce/2006/mfsa2006-45.html
http://www.mozilla.org/security/announce/2006/mfsa2006-46.html
http://www.mozilla.org/security/announce/2006/mfsa2006-47.html
http://www.mozilla.org/security/announce/2006/mfsa2006-48.html
http://www.mozilla.org/security/announce/2006/mfsa2006-50.html
http://www.mozilla.org/security/announce/2006/mfsa2006-51.html
http://www.mozilla.org/security/announce/2006/mfsa2006-52.html
http://www.mozilla.org/security/announce/2006/mfsa2006-53.html
http://www.mozilla.org/security/announce/2006/mfsa2006-54.html
http://www.mozilla.org/security/announce/2006/mfsa2006-55.html
http://www.mozilla.org/security/announce/2006/mfsa2006-56.html

Sun Solaris ACK Storm Denial of Service Vulnerability
“Denial of Service”

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

The vulnerability is caused due to an error in the handling of TCP packets with incorrect

sequence numbers, which can be exploited to cause a so-called "ACK Storm" where two systems try to re-synchronize the TCP session indefinitely.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102206-1

Sun Solaris IP Implementation Routing Table Bypass

"Bypass the routing table"

A vulnerability has been reported in Solaris, which can be exploited by malicious, local users to bypass certain restrictions.

The vulnerability is caused due to an error in the IP implementation, which makes it possible to bypass the routing table and send packets to/through an on-link router other than the defined one.

Successful exploitation may allow access to services otherwise not reachable and bypassing of firewall rules.

The vulnerability affects Solaris 10 with patches 118833-06 through 118833-17 (SPARC) or patches 118855-04 through 118855-14 (x86).

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102509-1

rPath update for sendmail

"Denial of Service"

rPath has issued an update for sendmail. This fixes a vulnerability, which can be exploited by malicious people to cause a DoS (Denial of Service).

References:
https://issues.rpath.com/browse/RPL-526

Novell Client Firewall Privilege Escalation Vulnerability

"Gain escalated privileges"

A vulnerability has been discovered in Novell Client Firewall, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to the application windows running with SYSTEM privileges and not properly restricting users from running arbitrary programs. This can be exploited to execute arbitrary commands with SYSTEM privileges by e.g. crafting a batch file executing cmd.exe and then move another file over this file inside Explorer via the "Save Configuration As..." functionality or similar.

The vulnerability has been confirmed in version 2.0 Build 0727. Other versions may also be affected.

References:
http://secunia.com/advisories/21161/

Sun Solaris sysinfo() Kernel Memory Disclosure
"Gain knowledge of potentially sensitive information"

A vulnerability has been reported in Solaris, which can be exploited by malicious, local users to gain knowledge of potentially sensitive information.

The vulnerability is caused due to an integer underflow error in the "sysinfo()" system call and makes it possible to partially disclose contents in kernel memory.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102343-1
http://www.idefense.com/intelligence/vulnerabilities/display.php?id=410

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