

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

[Apache Chunked Vulnerability Scanner](#) - The S4 Apache Chunked Vulnerability 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 Apache Chunked Encoding buffer overflow.

Download Here:

<http://www.netvigilance.com/productdownloads?productname=apachechunkedvulnerabilityscanner>

With so many vendors in the Vulnerability Management and Assessment market, it can be very hard to make the right choice.

That's why netVigilance is making that choice a lot easier.

Just a couple of months ago, we won SC Magazine's coveted Innovator of the Year award for 2010: see <http://bit.ly/hAoPP5> for the full article (SC Magazine free registration required).

And now our industry-leading solutions have been honored again.

That's why we are especially pleased to announce that netVigilance Internal Scan (Cloud) has won the prestigious SC Magazine "Best Buy" award in the "Vulnerability Assessment" category. (See the entire article here <http://bit.ly/eiEruz>)

This award is based on objective testing and in-depth, independent evaluations. Ultimately, we beat out each and every one of our competitors to take top honors:

Core Impact

Critical Watch

Cyberim/DragonSoft

eEye Retina

GFI Languard

Lumension Scan

ManageEngine

McAfee Vulnerability Manager

Saint

SecPoint

Tenable Network Security

Now is the time to let netVigilance take your organization's vulnerability detection, assessment and remediation processes Beyond Compliance™.

Before you renew with one of those other vendors – or if your need for vulnerability detection and assessment is a new one -- be sure to call netVigilance, SC Magazine 2010 Innovator of the Year and 2011 "Best Buy."

Our industry-leading, award-winning solutions are comprehensive and used by Global 1000 companies in all of the following areas:

- **Internal Scanning** (netVigilance Internal Scan)
- **External Scanning** (netVigilance External Scan)
- **PCI-DSS ASV Testing** (netVigilance PCI Scan)
- **Web Application Scanning** (netVigilance Web Scan)
- **Remote Manual Penetration Testing**

Don't wait to take your company Beyond Compliance™ in 2011. Call or email us today.

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

• **PWC interview: Security lessons in the cloud**

CSO - CSO recently interviewed Gary Loveland, a principal in PricewaterhouseCooper's advisory practice and head of the firm's global security practice, about the latest in cloud security issues. Loveland has functioned as a data security officer and has recommended and implemented security strategies in large-scale business environments.

CSO: What do you consider to be the most serious security threats related to cloud computing? Loveland: One of the most serious security threats to cloud computing is the fact that it is still an emerging technology, and even savvy IT leaders may not fully understand how the multiple layers of technology that comprise the "cloud" work together. Leveraging use case scenarios about specific risks and threats can be very helpful, so that [executives] can see more clearly where they are at risk and better understand how they can mitigate it. For example, multi-tenancy environments pose a threat at several layers, such as the complexity of the rule sets that drive routing and access to domain resources. A misconfiguration can result in unauthorized access to privileged information. Computerworld

Full Story :

http://www.computerworld.com/s/article/9207578/PWC_interview_Security_lessons_in_the_cloud?source=rss_security

• **Waledac botnet poised for a rebound with stolen credentials**

IDG News Service - The Waledac botnet, crippled by legal action from Microsoft and covert infiltration by security researchers just a year ago, appears poised for a big comeback.

Waledac was mostly shut down after Microsoft -- whose Hotmail service had been abused by the botnet -- was granted a temporary restraining order by a U.S. court that shut down domain names the botnet used to communicate. Security researchers also managed to disrupt Waledac's peer-to-peer communications system and gain control over some 60,000 infected computers.

But according to researchers from security vendor Last Line, Waledac has collected 489,528 credentials for POP3 e-mail accounts, which will likely be used for high-quality spam campaigns. Computerworld

Full Story :

http://www.computerworld.com/s/article/9207780/Waledac_botnet_poised_for_a_rebound_with_stolen_credentials?

• Next-generation banking malware emerges after Zeus

IDG News Service - The rumored combination of two pieces of advanced online banking malware appears to be fully underway after several months of speculation.

What appears to be a beta version of a piece of malware that has bits of both Zeus and SpyEye is now in circulation, albeit among just a few people, said Aviv Raff, CTO and cofounder of Seculert.

Seculert has published screen shots of the new malware, which has two versions of a control panel used for managing infected computers. One of those control panels resembles one in Zeus, and the other resembles that in SpyEye. Both of the control panels are connected to the same back-end command-and-control server, he said. Computerworld

Full Story :

http://www.computerworld.com/s/article/9207940/Next_generation_banking_malware_emerges_after_Zeus?source=r

• The Internet kill switch that isn't

IDG News Service - A cybersecurity proposal in the U.S. Congress, called an "Internet kill switch" plan by some critics, isn't exactly what that sounds like.

Plans by members of the U.S. Senate Homeland Security and Government Affairs Committee to reintroduce 2010's Protecting Cyberspace as a National Asset Act have led some critics to compare provisions in the bill to the Egyptian government's order to shut down all Internet access across the country during recent protests.

But the Egypt comparison -- and the term "Internet kill switch" -- is a stretch. Still, some tech and civil liberties groups have questioned the powers the proposal would give the president. Computerworld

Full Story :

http://www.computerworld.com/s/article/9207980/The_Internet_kill_switch_that_isn_t?source=rss_security

New Vulnerabilities Tested in SecureScout

• 13780 Oracle Database Server - Client System Analyzer component unspecified Vulnerability (jan-2011/CVE-2010-3600)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Client System Analyzer" component.

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

References:

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-11-018/>

* CONFIRM:

<http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html>

* BID: 45883

<http://www.securityfocus.com/bid/45883>

* SECTRACK: 1024972

<http://www.securitytracker.com/id?1024972>

* SECUNIA: 42895

<http://secunia.com/advisories/42895>

* SECUNIA: 42921

<http://secunia.com/advisories/42921>

* VUPEN: ADV-2011-0139

<http://www.vupen.com/english/advisories/2011/0139>

* VUPEN: ADV-2011-0140

<http://www.vupen.com/english/advisories/2011/0140>

* XF: oracle-db-gridcontrol-unspecified(64755)

<http://xforce.iss.net/xforce/xfdb/64755>

CVE Reference:

CVE-2010-3600 (cve.mitre.org, nvd.nist.gov)

• 13781 Oracle Database Server - Cluster Verify Utility component unspecified Vulnerability (jan-2011/CVE-2010-4423)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Cluster Verify Utility" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html>
- * BID: 45859
<http://www.securityfocus.com/bid/45859>
- * SECTRACK: 1024972
<http://www.securitytracker.com/id?1024972>
- * SECUNIA: 42895
<http://secunia.com/advisories/42895>
- * VUPEN: ADV-2011-0139
<http://www.vupen.com/english/advisories/2011/0139>
- * XF: oracle-db-cluster-priv-escalation(64756)
<http://xforce.iss.net/xforce/xfdb/64756>

CVE Reference:

CVE-2010-4423 (cve.mitre.org, nvd.nist.gov)

● **13782 Oracle Database Server - Database Vault component unspecified Vulnerability (jan-2011/CVE-2010-4421)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Database Vault" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html>
- * BID: 45905
<http://www.securityfocus.com/bid/45905>
- * SECTRACK: 1024972
<http://www.securitytracker.com/id?1024972>
- * SECUNIA: 42895
<http://secunia.com/advisories/42895>
- * VUPEN: ADV-2011-0139
<http://www.vupen.com/english/advisories/2011/0139>
- * XF: oracle-db-databasevault-unspecified(64757)
<http://xforce.iss.net/xforce/xfdb/64757>

CVE Reference:

CVE-2010-4421 (cve.mitre.org, nvd.nist.gov)

● **13783 Oracle Database Server - Oracle Spatial component unspecified Vulnerability (jan-2011/CVE-2010-3590)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Oracle Spatial" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html>
- * BID: 45880
<http://www.securityfocus.com/bid/45880>
- * SECTRACK: 1024972
<http://www.securitytracker.com/id?1024972>
- * SECUNIA: 42895
<http://secunia.com/advisories/42895>
- * VUPEN: ADV-2011-0139
<http://www.vupen.com/english/advisories/2011/0139>
- * XF: oracle-db-oracle-spatial-unspec(64758)
<http://xforce.iss.net/xforce/xfdb/64758>

CVE Reference:

CVE-2010-3590 (cve.mitre.org, nvd.nist.gov)

● **13784 Oracle Database Server - Scheduler Agent component unspecified Vulnerability (jan-2011/CVE-2010-4413)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Scheduler Agent" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html>
- * BID: 45845
<http://www.securityfocus.com/bid/45845>
- * SECTRACK: 1024972
<http://www.securitytracker.com/id?1024972>
- * SECUNIA: 42895
<http://secunia.com/advisories/42895>
- * VUPEN: ADV-2011-0139
<http://www.vupen.com/english/advisories/2011/0139>
- * XF: oracle-db-scheduler-agent-unspec(64759)
<http://xforce.iss.net/xforce/xfdb/64759>

CVE Reference:

CVE-2010-4413 (cve.mitre.org, nvd.nist.gov)

● **13785 Oracle Database Server - Database Vault component unspecified Vulnerability (jan-2011/CVE-2010-4420)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Database Vault" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html>
- * BID: 45855
<http://www.securityfocus.com/bid/45855>
- * SECTRACK: 1024972
<http://www.securitytracker.com/id?1024972>
- * SECUNIA: 42895
<http://secunia.com/advisories/42895>
- * VUPEN: ADV-2011-0139
<http://www.vupen.com/english/advisories/2011/0139>
- * XF: oracle-db-vault-unspecified(64760)
<http://xforce.iss.net/xforce/xfdb/64760>

CVE Reference:

CVE-2010-4420 (cve.mitre.org, nvd.nist.gov)

● **19183 PHP 'zend_strtod()' Function Floating-Point Value Denial of Service Vulnerability**

strtod.c, as used in the zend_strtod function in PHP 5.2 before 5.2.17 and 5.3 before 5.3.5, and other products, allows context-dependent attackers to cause a denial of service (infinite loop) via a certain floating-point value in scientific notation, which is not properly handled in x87 FPU registers.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS** Risk: **Medium**

References:

- * MLIST: [oss-security] 20110105 Re: possible flaw in widely used strtod.c implementation
<http://www.openwall.com/lists/oss-security/2011/01/05/8>
- * MLIST: [oss-security] 20110105 possible flaw in widely used strtod.c implementation
<http://www.openwall.com/lists/oss-security/2011/01/05/2>
- * MLIST: [oss-security] 20110106 Re: possible flaw in widely used strtod.c implementation
<http://www.openwall.com/lists/oss-security/2011/01/06/5>
- * MISC:
<http://hal.archives-ouvertes.fr/docs/00/28/14/29/PDF/floating-point-article.pdf>
- * MISC:
http://svn.php.net/viewvc/php/php-src/branches/PHP_5_2/Zend/zend_strtod.c?r1=266327&pathrev=307095&r2=307095&pathrev=307095
- * MISC:
<http://www.exploringbinary.com/php-hangs-on-numeric-value-2-2250738585072011e-308/>

* CONFIRM:

<http://bugs.php.net/53632>

* SLACKWARE: SSA:2011-010-01

<http://slackware.com/security/viewer.php?l=slackware-security&v=2011&m=slackware-security.484686>

* UBUNTU: USN-1042-1

<http://www.ubuntu.com/usn/USN-1042-1>

* BID: 45668

<http://www.securityfocus.com/bid/45668>

* SECUNIA: 42843

<http://secunia.com/advisories/42843>

* SECUNIA: 42812

<http://secunia.com/advisories/42812>

* VUPEN: ADV-2011-0060

<http://www.vupen.com/english/advisories/2011/0060>

* VUPEN: ADV-2011-0066

<http://www.vupen.com/english/advisories/2011/0066>

* VUPEN: ADV-2011-0077

<http://www.vupen.com/english/advisories/2011/0077>

* XF: php-zendstrtod-dos(64470)

<http://xforce.iss.net/xforce/xfdb/64470>

CVE Reference:

CVE-2010-4645 (cve.mitre.org, nvd.nist.gov)

• 19184 Netlogon RPC Null dereference DOS Vulnerability (MS10-101/2207559) (Remote File Checking)

A remote authenticated denial of service vulnerability exists in implementations of the Netlogon RPC Service on affected versions of Windows Server. An attacker who successfully exploited this vulnerability could cause affected versions of the Windows Server to restart.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Crash** Risk: **Medium**

References:

* MS: MS10-101

<http://www.microsoft.com/technet/security/Bulletin/MS10-101.msp>

* CERT: TA10-348A

<http://www.us-cert.gov/cas/techalerts/TA10-348A.html>

* SECTRACK: 1024883

<http://www.securitytracker.com/id?1024883>

* BID: 45271

<http://www.securityfocus.com/bid/45271>

* VUPEN: VUPEN/ADV-2010-3223

<http://www.vupen.com/english/advisories/2010/3223>

CVE Reference:

CVE-2010-2742 (cve.mitre.org, nvd.nist.gov)

• 19185 Task Scheduler Vulnerability (MS10-092/2305420) (Remote File Checking)

An elevation of privilege vulnerability exists in the way that the Windows Task Scheduler improperly validates whether scheduled tasks run within the intended security context. An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

* BID: 44357

<http://www.securityfocus.com/bid/44357>

* VUPEN: VUPEN/ADV-2010-2761

<http://www.vupen.com/english/advisories/2010/2761>

* MS: MS10-092

<http://www.microsoft.com/technet/security/Bulletin/MS10-092.msp>

* CERT: TA10-348A

<http://www.us-cert.gov/cas/techalerts/TA10-348A.html>

* SECTRACK: 1024874

<http://www.securitytracker.com/id?1024874>

CVE Reference:

CONFIRM: <http://blogs.technet.com/b/msrc/archive/2011/01/28/microsoft-releases-security-advisory-2501696.aspx>

CVE Reference: [CVE-2011-0096](#)

• **CVE-2010-3854 Apache CVSS 2.0 Score = 4.3**

Multiple cross-site scripting (XSS) vulnerabilities in the web administration interface (aka Futon) in Apache CouchDB 0.8.0 through 1.0.1 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

XF: <http://xforce.iss.net/xforce/xfdb/65050>

VUPEN: <http://www.vupen.com/english/advisories/2011/0263>

SECTRAK: <http://www.securitytracker.com/id?1025013>

BID: <http://www.securityfocus.com/bid/46066>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/516058/100/0/threaded>

SECUNIA: <http://secunia.com/advisories/43111>

MLIST:

http://mail-archives.apache.org/mod_mbox/couchdb-dev/201101.mbox/%3CC840F655-C8C5-4EC6-8AA8-DD223E39C34

CVE Reference: [CVE-2010-3854](#)

• **CVE-2011-0276 HP CVSS 2.0 Score = 10.0**

HP OpenView Performance Insight Server 5.2, 5.3, 5.31, 5.4, and 5.41 contains a "hidden account" in the com.trinagy.security.XMLUserManager Java class, which allows remote attackers to execute arbitrary code via the doPost method in the com.trinagy.servlet.HelpManagerServlet class.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

XF: <http://xforce.iss.net/xforce/xfdb/65038>

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-11-034>

VUPEN: <http://www.vupen.com/english/advisories/2011/0258>

SECTRAK: <http://www.securitytracker.com/id?1025014>

BID: <http://www.securityfocus.com/bid/46079>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/516093/100/0/threaded>

SECUNIA: <http://secunia.com/advisories/43145>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02695453>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02695453>

CVE Reference: [CVE-2011-0276](#)

• **CVE-2010-0110 Symantec CVSS 2.0 Score = 9.3**

Multiple stack-based buffer overflows in Intel Alert Management System (aka AMS or AMS2), as used in Symantec AntiVirus Corporate Edition (SAVCE) 10.x before 10.1 MR10, Symantec System Center (SSC) 10.x, and Symantec Quarantine Server 3.5 and 3.6, allow remote attackers to execute arbitrary code via (1) a long string to msgsys.exe, related to the AMSSendAlertAct function in AMSLIB.dll in the Intel Alert Handler service (aka Symantec Intel Handler service); a long (2) modem string or (3) PIN number to msgsys.exe, related to pagehdl.dll in the Intel Alert Handler service; or (4) a message to msgsys.exe, related to iao.exe in the Intel Alert Originator service.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-11-032>

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-11-031>

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-11-030>

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-11-028>

VUPEN: <http://www.vupen.com/english/advisories/2011/0234>

CONFIRM:

http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory

BID: <http://www.securityfocus.com/bid/45936>

SECTRAK: <http://securitytracker.com/id?1024996>

SECUNIA: <http://secunia.com/advisories/43106>

SECUNIA: <http://secunia.com/advisories/43099>

CVE Reference: [CVE-2010-0110](#)

• **CVE-2010-0111 Symantec CVSS 2.0 Score = 9.3**

HDNLR SVC.EXE in the Intel Alert Handler service (aka Symantec Intel Handler service) in Intel Alert Management System (aka AMS or AMS2), as used in Symantec AntiVirus Corporate Edition (SAVCE) 10.x before 10.1 MR10, Symantec System Center (SSC) 10.x, and Symantec Quarantine Server 3.5 and 3.6, allows remote attackers to execute arbitrary programs by sending msgsys.exe a UNC share pathname, which is used directly in a CreateProcessA (aka CreateProcess) call.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

XF: <http://xforce.iss.net/xforce/xfdb/64943>

XF: <http://xforce.iss.net/xforce/xfdb/64942>

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-11-029>

VUPEN: <http://www.vupen.com/english/advisories/2011/0234>

CONFIRM:

http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory

BID: <http://www.securityfocus.com/bid/45935>

SECTRAK: <http://securitytracker.com/id?1024997>

SECUNIA: <http://secunia.com/advisories/43106>

SECUNIA: <http://secunia.com/advisories/43099>

CVE Reference: [CVE-2010-0111](#)

• **CVE-2011-0688 Symantec CVSS 2.0 Score = 9.3**

Intel Alert Management System (aka AMS or AMS2), as used in Symantec Antivirus Corporate Edition (SAVCE) 10.x before 10.1 MR10, Symantec System Center (SSC) 10.x, and Symantec Quarantine Server 3.5 and 3.6, allows remote attackers to execute arbitrary commands via crafted messages over TCP, as discovered by Junaid Bohio, a different vulnerability than CVE-2010-0110 and CVE-2010-0111. NOTE: some of these details are obtained from third party information.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

VUPEN: <http://www.vupen.com/english/advisories/2011/0234>

CONFIRM:

http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory

BID: <http://www.securityfocus.com/bid/45936>

SECTRAK: <http://securitytracker.com/id?1024996>

SECUNIA: <http://secunia.com/advisories/43099>

CVE Reference: [CVE-2011-0688](#)

• **CVE-2010-3719 Symantec CVSS 2.0 Score = 8.5**

Eval injection vulnerability in IMAdminSchedTask.asp in the administrative interface for Symantec IM Manager 8.4.16 and earlier allows remote attackers to execute arbitrary code via unspecified parameters to the ScheduleTask method.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

XF: <http://xforce.iss.net/xforce/xfdb/65040>

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-11-037>

VUPEN: <http://www.vupen.com/english/advisories/2011/0259>

CONFIRM:

http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory

BID: <http://www.securityfocus.com/bid/45946>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/516103/100/0/threaded>

SECUNIA: <http://secunia.com/advisories/43143>

CVE Reference: [CVE-2010-3719](#)

• **CVE-2011-0732 IBM CVSS 2.0 Score = 10.0**

Multiple unspecified vulnerabilities in IBM Tivoli Integrated Portal (TIP) 1.1.1.1, as used in IBM Tivoli Common Reporting (TCR) 1.2.0 before Interim Fix 9, have unknown impact and attack vectors, related to "security vulnerabilities of Websphere Application Server bundled within" and "many internal defects and APARs."

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=swg11Y99978>

SECUNIA: <http://secunia.com/advisories/43030>

CVE Reference: [CVE-2011-0732](#)

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