ScoutNews
The weekly Security update from the makers of SecureScout
September 11, 2009

2009 Issue #37

Table of Contents

Product Focus

Winny (WinNY) software Scanner - The S4 Winny Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if the peer-to-peer software Winny is installed and running.

Download Here:
http://www.netvigilance.com/productdownloads?productname=winnyscanner

This Week in Review

Protect your data! web site malware increasing. And getting more sophisticated. Should the president have the power to shut down the internet?

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

- **End-to-End Encryption: The PCI Security Holy Grail**

CSO - One of the fascinating things to do when in New York City is to visit the Federal Reserve gold vault. The vault lies 86 feet below sea level, resting on Manhattan bedrock, and holds approximately 5,000 metric tons of gold bullion. The Federal Reserve Bank does not own the gold but serves as guardian of the precious metal, which it protects at no charge as a gesture of goodwill to other nations.

Obviously, the security measures to protect hundreds of billions of dollars of gold are intense. But even if a thief were to breach the underground defenses and avoid the marksmen, how would he get the gold out? Gold is dense, difficult to transport and heavy, with each bar weighing approximately 27 pounds. Combined with the impossible-to-negotiate downtown Manhattan traffic, those facts contribute to the vault being a safe and sound way to protect the gold.
Computerworld

Full Story :
http://www.computerworld.com/s/article/9137827/End_to_End_Encryption_The_PCI_Security_Holy_Grail?source=rs

- **7 Reasons Websites Are No Longer Safe**

CSO - Conventional wisdom is that Web wanderers are safe as long as they avoid sites that serve up pornography, stock tips, games and the like. But according to recently gathered research from Boston-based IT security and control firm Sophos, sites we take for granted are not as secure as they appear.

Among the findings in Sophos' threat report for the first six months of this year, 23,500 new infected Web pages -- one every 3.6 seconds -- were detected each day during that period. That's four times worse than the same period last year, said Richard Wang, who manages the Boston lab. Many such infections were found on legitimate websites.

In a recent interview with CSOonline, Wang outlined seven primary reasons legitimate sites are becoming more dangerous. Computerworld

Full Story :
http://www.computerworld.com/s/article/9137767/7_Reasons_Websites_Are_No_Longer_Safe?source=rss_security

- **Threat of the Month -- Conficker**

Conficker, which is both a worm and a bot, is one of the more sophisticated pieces of malicious software (malware) we have seen to date. SC Magazine

Full Story :
http://www.scmagazineus.com/pages/Login.aspx?retUrl=/Threat-of-the-Month--Conficker/article/148534/&PageTypeI

- **Federal IT strategy, hope over reality**

Network World - A few weeks ago I wrote a column about the Internet Kill Switch, a really, really bad idea that was mooted in a draft bill put forward by Sen. John Rockefeller (D-W.Va.), chairman of the Senate Committee on Commerce, Science and Transportation.

Lawmakers strike new tone with proposed bill

The purpose of this bill was to give the president the ability to declare "a cybersecurity emergency and order the limitation or shutdown of Internet traffic to and from any compromised Federal government or United States critical infrastructure information system or network". This bill was a triumph of hope over reality and, for so many reasons, a very bad idea. Computerworld

Full Story :
http://www.computerworld.com/s/article/9137638/Federal_IT_strategy_hope_over_reality?source=rss_security

New Vulnerabilities Tested in SecureScout

- **18501 JScript Remote Code Execution Vulnerability (MS09-045/971961) (Remote File Checking)**

A remote code execution vulnerability exists in the way that the JScript scripting engine processes scripts in Web pages. The vulnerability could allow remote code execution if a user opened a specially crafted file or visited a Web site that is running a specially crafted script. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* MS: MS09-045
http://www.microsoft.com/technet/security/Bulletin/MS09-045.mspx
* BID: 36224
http://www.securityfocus.com/bid/36224

CVE Reference:

CVE-2009-1920 (cve.mitre.org, nvd.nist.gov)

- **18502 Wireless Frame Parsing Remote Code Execution Vulnerability (MS09-049/970710) (Remote File Checking)**

A remote code execution vulnerability exists in the way that the Wireless LAN AutoConfig Service (wlansvc) parses specific frames received on the wireless network. This vulnerability could allow remote code execution if a client or server with a wireless network interface enabled receives specially crafted wireless frames. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full

user rights.

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

References:

* MS: MS09-049
http://www.microsoft.com/technet/security/Bulletin/MS09-049.mspx
* BID: 36223
http://www.securityfocus.com/bid/36223

CVE Reference:

CVE-2009-1132 (cve.mitre.org, nvd.nist.gov)

• 18503 Windows Media Header Parsing Invalid Free Vulnerability (MS09-047/973812) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Windows handles specially crafted ASF format files. This vulnerability could allow remote code execution if a user opened a specially crafted file. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* MS: MS09-047
http://www.microsoft.com/technet/security/Bulletin/MS09-047.mspx
* BID: 36225
http://www.securityfocus.com/bid/36225

CVE Reference:

CVE-2009-2498 (cve.mitre.org, nvd.nist.gov)

• 18504 Windows Media Playback Memory Corruption Vulnerability (MS09-047/973812) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Windows handles MP3 media files. This vulnerability could allow remote code execution if a user opened a specially crafted file. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* MS: MS09-047
http://www.microsoft.com/technet/security/Bulletin/MS09-047.mspx
* BID: 36228
http://www.securityfocus.com/bid/36228

CVE Reference:

CVE-2009-2499 (cve.mitre.org, nvd.nist.gov)

• 18505 TCP/IP Zero Window Size Vulnerability (MS09-048/967723) (Remote File Checking)

A denial of service vulnerability exists in TCP/IP processing in Microsoft Windows due to the way that Windows handles an excessive number of established TCP connections. The effect of this vulnerability can be amplified by the requirement to process specially crafted packets with a TCP receive window size set to a very small value or zero. An attacker could exploit the vulnerability by flooding a system with specially crafted packets causing the affected system to stop responding to new requests or automatically restart.

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

References:

* MLIST: [dailydave] 20081002 TCP Resource Exhaustion DoS Attack Speculation
http://lists.immunitysec.com/pipermail/dailydave/2008-October/005360.html
* MISC:

http://blog.robertlee.name/2008/10/conjecture-speculation.html
* MISC:
http://searchsecurity.techtarget.com.au/articles/27154-TCP-is-fundamentally-borked
* MISC:
http://www.outpost24.com/news/news-2008-10-02.html
* MISC:
https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html
* CISCO: 20081017 Cisco Response to Outpost24 TCP State Table Manipulation Denial of Service Vulnerabilities
http://www.cisco.com/en/US/products/products_security_response09186a0080a15120.html
* CISCO: 20090908 TCP State Manipulation Denial of Service Vulnerabilities in Multiple Cisco Products
http://www.cisco.com/en/US/products/products_security_advisory09186a0080af511d.shtml
* MS: MS09-048
http://www.microsoft.com/technet/security/Bulletin/MS09-048.mspx

CVE Reference:

CVE-2008-4609 (cve.mitre.org, nvd.nist.gov)

• 18506 TCP/IP Timestamps Code Execution Vulnerability (MS09-048/967723) (Remote File Checking)

A remote code execution vulnerability exists in the Windows TCP/IP stack due to the TCP/IP stack not cleaning up state information correctly. This causes the TCP/IP stack to reference a field as a function pointer when it actually contains other information. An anonymous attacker could exploit the vulnerability by sending specially crafted TCP/IP packets to a computer that has a service listening over the network. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

* MS: MS09-048
http://www.microsoft.com/technet/security/Bulletin/MS09-048.mspx
* BID: 36265
http://www.securityfocus.com/bid/36265

CVE Reference:

CVE-2009-1925 (cve.mitre.org, nvd.nist.gov)

• 18507 TCP/IP Orphaned Connections Vulnerability (MS09-048/967723) (Remote File Checking)

A denial of service vulnerability exists in TCP/IP processing in Microsoft Windows due to an error in the processing of specially crafted packets with a small or zero TCP receive window size. If an application closes a TCP connection with pending data to be sent and an attacker has set a small or zero TCP receive window size, the affected server will not be able to completely close the TCP connection. An attacker could exploit the vulnerability by flooding a system with specially crafted packets causing the affected system to stop responding to new requests. The system would remain non-responsive even after the attacker stops sending malicious packets.

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

References:

* MS: MS09-048
http://www.microsoft.com/technet/security/Bulletin/MS09-048.mspx
* BID: 36269
http://www.securityfocus.com/bid/36269

CVE Reference:

CVE-2009-1926 (cve.mitre.org, nvd.nist.gov)

• 18508 DHTML Editing Component ActiveX Control Vulnerability (MS09-046/956844) (Remote File Checking)

A remote code execution vulnerability exists in the DHTML Editing Component ActiveX Control. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user.

If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* MS: MS09-046
http://www.microsoft.com/technet/security/Bulletin/MS09-046.mspx
* BID: 36280
http://www.securityfocus.com/bid/36280

CVE Reference:

CVE-2009-2519 (cve.mitre.org, nvd.nist.gov)

• 18509 PHP request with multiple dots Denial of Service Vulnerability

PHP 4.4.x before 4.4.9, and 5.x through 5.2.6, when used as a FastCGI module, allows remote attackers to cause a denial of service (crash) via a request with multiple dots preceding the extension, as demonstrated using foo..php.

The issue has been fixed in PHP versions 4.4.9 and 5.2.7.

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

References:

* BUGTRAQ: 20090302 rPSA-2009-0035-1 php php-cgi php-imap php-mcrypt php-mysql php-mysqli php-pgsql php-soap php-xsl php5 php5-cgi php5-imap php5-mcrypt php5-mysql php5-mysqli php5-pear php5-pgsql php5-soap php5-xsl
http://www.securityfocus.com/archive/1/archive/1/501376/100/0/threaded
* CONFIRM:
http://bugs.gentoo.org/show_bug.cgi?id=234102
* MLIST: [oss-security] 20080808 CVE request: php-5.2.6 overflow issues
http://www.openwall.com/lists/oss-security/2008/08/08/2
* MLIST: [oss-security] 20080813 Re: CVE request: php-5.2.6 overflow issues
http://www.openwall.com/lists/oss-security/2008/08/13/8
* CONFIRM:
http://wiki.rpath.com/Advisories:rPSA-2009-0035
* CONFIRM:
http://support.apple.com/kb/HT3549
* APPLE: APPLE-SA-2009-05-12
http://lists.apple.com/archives/security-announce/2009/May/msg00002.html
* DEBIAN: DSA-1647
http://www.debian.org/security/2008/dsa-1647
* FEDORA: FEDORA-2009-3768
https://www.redhat.com/archives/fedora-package-announce/2009-May/msg01451.html
* FEDORA: FEDORA-2009-3848
https://www.redhat.com/archives/fedora-package-announce/2009-May/msg01465.html
* HP: HPSBUX02431
http://marc.info/?l=bugtraq&m=124654546101607&w=2
* MANDRIVA: MDVSA-2009:021
http://www.mandriva.com/security/advisories?name=MDVSA-2009:021
* MANDRIVA: MDVSA-2009:022
http://www.mandriva.com/security/advisories?name=MDVSA-2009:022
* MANDRIVA: MDVSA-2009:023
http://www.mandriva.com/security/advisories?name=MDVSA-2009:023
* MANDRIVA: MDVSA-2009:024
http://www.mandriva.com/security/advisories?name=MDVSA-2009:024
* REDHAT: RHSA-2009:0350
http://www.redhat.com/support/errata/RHSA-2009-0350.html
* SUSE: SUSE-SR:2008:018
http://lists.opensuse.org/opensuse-security-announce/2008-09/msg00004.html
* CERT: TA09-133A
http://www.us-cert.gov/cas/techalerts/TA09-133A.html
* SECTRACK: 1020994
http://www.securitytracker.com/id?1020994
* SECUNIA: 32148
http://secunia.com/advisories/32148
* SECUNIA: 31982
http://secunia.com/advisories/31982
* SECUNIA: 35074
http://secunia.com/advisories/35074
* SECUNIA: 35306

http://secunia.com/advisories/35306
* SECUNIA: 35650
http://secunia.com/advisories/35650
* VUPEN: ADV-2008-2336
http://www.vupen.com/english/advisories/2008/2336
* VUPEN: ADV-2009-1297
http://www.vupen.com/english/advisories/2009/1297
* XF: php-curl-unspecified(44402)
http://xforce.iss.net/xforce/xfdb/44402
* BID: 31612
http://www.securityfocus.com/bid/31612

CVE Reference:

CVE-2008-3660 (cve.mitre.org, nvd.nist.gov)

- **18510 PHP rfc822_write_address arbitrary code execution Vulnerability**

php_imap.c in PHP 5.2.5, 5.2.6, 4.x, and other versions, uses obsolete API calls that allow context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long IMAP request, which triggers an "rfc822.c legacy routine buffer overflow" error message, related to the rfc822_write_address function.

The issue has been fixed in PHP versions 4.4.9 and 5.2.7.

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

References:

* BUGTRAQ: 20090302 rPSA-2009-0035-1 php php-cgi php-imap php-mcrypt php-mysql php-mysqli php-pgsql php-soap php-xsl php5 php5-cgi php5-imap php5-mcrypt php5-mysql php5-mysqli php5-pear php5-pgsql php5-soap php5-xsl
http://www.securityfocus.com/archive/1/archive/1/501376/100/0/threaded
* MISC:
http://bugs.php.net/bug.php?id=42862
* CONFIRM:
https://bugs.gentoo.org/show_bug.cgi?id=221969
* MLIST: [oss-security] 20080619 CVE request: php 5.2.6 ext/imap buffer overflows
http://www.openwall.com/lists/oss-security/2008/06/19/6
* MLIST: [oss-security] 20080624 Re: CVE request: php 5.2.6 ext/imap buffer overflows
http://www.openwall.com/lists/oss-security/2008/06/24/2
* CONFIRM:
http://wiki.rpath.com/Advisories:rPSA-2009-0035
* CONFIRM:
http://support.apple.com/kb/HT3549
* APPLE: APPLE-SA-2009-05-12
http://lists.apple.com/archives/security-announce/2009/May/msg00002.html
* FEDORA: FEDORA-2009-3768
https://www.redhat.com/archives/fedora-package-announce/2009-May/msg01451.html
* FEDORA: FEDORA-2009-3848
https://www.redhat.com/archives/fedora-package-announce/2009-May/msg01465.html
* HP: HPSBUX02431
http://marc.info/?l=bugtraq&m=124654546101607&w=2
* MANDRIVA: MDVSA-2008:126
http://www.mandriva.com/security/advisories?name=MDVSA-2008:126
* MANDRIVA: MDVSA-2008:127
http://www.mandriva.com/security/advisories?name=MDVSA-2008:127
* MANDRIVA: MDVSA-2008:128
http://www.mandriva.com/security/advisories?name=MDVSA-2008:128
* SUSE: SUSE-SR:2008:027
http://lists.opensuse.org/opensuse-security-announce/2008-12/msg00002.html
* UBUNTU: USN-628-1
http://www.ubuntu.com/usn/usn-628-1
* CERT: TA09-133A
http://www.us-cert.gov/cas/techalerts/TA09-133A.html
* BID: 29829
http://www.securityfocus.com/bid/29829
* OSVDB: 46641
http://osvdb.org/46641
* SECUNIA: 31200
http://secunia.com/advisories/31200
* SECUNIA: 35074

http://secunia.com/advisories/35074
* SECUNIA: 35306
http://secunia.com/advisories/35306
* SECUNIA: 35650
http://secunia.com/advisories/35650
* VUPEN: ADV-2009-1297
http://www.vupen.com/english/advisories/2009/1297
* XF: php-phpimap-dos(43357)
http://xforce.iss.net/xforce/xfdb/43357

CVE Reference:

CVE-2008-2829 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-1925 Microsoft CVSS 2.0 Score = 10.0

The TCP/IP implementation in Microsoft Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2 does not properly manage state information, which allows remote attackers to execute arbitrary code by sending packets to a listening service, and thereby triggering misinterpretation of an unspecified field as a function pointer, aka "TCP/IP Timestamps Code Execution Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-048.mspx

CVE Reference: CVE-2009-1925

• CVE-2009-1132 Microsoft CVSS 2.0 Score = 9.3

Heap-based buffer overflow in the Wireless LAN AutoConfig Service (aka Wlansvc) in Microsoft Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via a malformed wireless frame, aka "Wireless Frame Parsing Remote Code Execution Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-049.mspx

CVE Reference: CVE-2009-1132

• CVE-2009-1920 Microsoft CVSS 2.0 Score = 9.3

The JScript scripting engine 5.1, 5.6, 5.7, and 5.8 in JScript.dll in Microsoft Windows, as used in Internet Explorer, does not properly load decoded scripts into memory before execution, which allows remote attackers to execute arbitrary code via a crafted web site that triggers memory corruption, aka "JScript Remote Code Execution Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-045.mspx

CVE Reference: CVE-2009-1920

• CVE-2009-2498 Microsoft CVSS 2.0 Score = 9.3

Microsoft Windows Media Format Runtime 9.0, 9.5, and 11 and Windows Media Services 9.1 and 2008 do not properly parse malformed headers in Advanced Systems Format (ASF) files, which allows remote attackers to execute arbitrary code via a crafted (1) .asf, (2) .wmv, or (3) .wma file, aka "Windows Media Header Parsing Invalid Free Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-047.mspx

CVE Reference: CVE-2009-2498

- **CVE-2009-2499 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Windows Media Format Runtime 9.0, 9.5, and 11; and Microsoft Media Foundation on Windows Vista Gold, SP1, and SP2 and Server 2008; allows remote attackers to execute arbitrary code via an MP3 file with crafted metadata that triggers memory corruption, aka "Windows Media Playback Memory Corruption Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-047.mspx

CVE Reference: CVE-2009-2499

- **CVE-2009-2519 Microsoft CVSS 2.0 Score = 9.3**

The DHTML Editing Component ActiveX control in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 does not properly format HTML markup, which allows remote attackers to execute arbitrary code via a crafted web site that triggers "system state" corruption, aka "DHTML Editing Component ActiveX Control Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-046.mspx

CVE Reference: CVE-2009-2519

- **CVE-2009-1926 Microsoft CVSS 2.0 Score = 7.8**

Microsoft Windows 2000 SP4, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allow remote attackers to cause a denial of service (TCP outage) via a series of TCP sessions that have pending data and a (1) small or (2) zero receive window size, and remain in the FIN-WAIT-1 or FIN-WAIT-2 state indefinitely, aka "TCP/IP Orphaned Connections Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-048.mspx

CVE Reference: CVE-2009-1926

- **CVE-2009-3103 Microsoft CVSS 2.0 Score = 7.8**

Array index error in the SMB2 protocol implementation in srv2.sys in Microsoft Windows 7, Server 2008, and Vista Gold, SP1, and SP2 allows remote attackers to cause a denial of service (system crash) via an & (ampersand) character in a Process ID High header field in a NEGOTIATE PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memory location. NOTE: some of these details are obtained from third party information.

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

References:

BID: http://www.securityfocus.com/bid/36299

SECUNIA: http://secunia.com/advisories/36623

MISC: http://isc.sans.org/diary.html?storyid=7093

MISC: http://g-laurent.blogspot.com/2009/09/windows-vista7-smb20-negotiate-protocol.html

FULLDISC: http://archives.neohapsis.com/archives/fulldisclosure/2009-09/0090.html

CVE Reference: CVE-2009-3103

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