ScoutNews
The weekly Security update from the makers of SecureScout
June 04, 2010

2010 Issue #23

Table of Contents

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

This Week in Review

U.S. to update security policies. Microsoft to fix 34 holes. MAC owners be aware of spyware. Software company not allowed to market product as undetectable.

SecureScout Windows Edition runs on Windows 7, Vista, Windows Server 2008 and the new Installer with support for the new operating systems is now available on the password protected download site.

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

- **U.S. cybersecurity policies close to major update**

The U.S. House of Representatives has passed a defense bill that contains an amendment aimed at regulating the information security responsibilities and practices of federal agencies.

The amendment, sponsored by Rep. Jim Langevin, D-R.I., and Rep. Diane Watson, D-Calif., updates the Federal Information Security Management Act (FISMA) and establishes a National Office for Cyberspace in the Executive Office of the President.

The amendment was attached to the National Defense Authorization Act for Fiscal Year 2011, which passed the House Friday by a 229-186 vote. SC Magazine

Full Story :
http://www.scmagazineus.com/us-cybersecurity-policies-close-to-major-update/article/171586/?utm_source=feedbur

- **Microsoft to fix 34 holes in Windows, Office, IE**

Microsoft will on Tuesday issue 10 bulletins fixing 34 vulnerabilities affecting Windows, Office, and Internet Explorer.

Six of the bulletins affect Windows, with two of those rated critical by Microsoft. Two bulletins target Office, one targets both Windows and Office, and one critical bulletin affects Internet Explorer, according to a Microsoft Security Response Center blog post on Thursday.

Microsoft also said that with the June bulletins it will be closing Security Advisory 983438, which involves a vulnerability in SharePoint Services 3.0 and SharePoint Server 2007 that was disclosed in late April and which could lead to a cross-site scripting attack via the browser. Proof-of-concept exploit code has been published for that. Cnet Security

Full Story :
http://news.cnet.com/8301-27080_3-20006781-245.html?part=rss&subj=news&tag=2547-1_3-0-20

- **Free apps install spyware on Macs**

Mac users downloading free screensavers and a video converter app from several popular download sites also got spyware that installs a back door, collects data, and sends encrypted information to remote servers, security company Intego said on Tuesday.

The high-risk spyware, dubbed OSX/OpinionSpy, was being installed along with nearly 30 screensavers developed by a company called 7art and an app called MishInc FLV to MP3, according to a list compiled by Intego.

They were found on Softpedia, MacUpdate, and CNET-owned VersionTracker, according to a post on Intego's Mac Security Blog. Cnet Security

Full Story :
http://news.cnet.com/8301-27080_3-20006502-245.html?part=rss&subj=news&tag=2547-1_3-0-20

- **FTC bars software maker from enabling illegal spying**

The Federal Trade Commission (FTC) has announced a settlement that bars an Orlando, Fla.-based company from marketing a spyware product as undetectable.

Under the settlement's terms, the result of a 2008 lawsuit filed by the FTC, CyberSpy Software is prohibited from "advertising that [its RemoteSpy keystroke logger] can be disguised and installed on someone's else's computer without the owner's knowledge."

The software must gain the approval of the computer owner before it can be installed, according to the settlement, announced Wednesday. SC Magazine

Full Story :
http://www.scmagazineus.com/ftc-bars-software-maker-from-enabling-illegal-spying/article/171668/?utm_source=fee

New Vulnerabilities Tested in SecureScout

- **12174 PostgreSQL NULL Character CA SSL Certificate Validation Security Bypass Vulnerability**

PostgreSQL 7.4.x before 7.4.27, 8.0.x before 8.0.23, 8.1.x before 8.1.19, 8.2.x before 8.2.15, 8.3.x before 8.3.9, and 8.4.x before 8.4.2 does not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based PostgreSQL servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended client-hostname restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

PostgreSQL versions prior to 7.4.27, 8.0.23, 8.1.19, 8.2.15, 8.3.9, 8.4.2 are vulnerable to this issue.

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

References:

* BUGTRAQ: 20100307 rPSA-2010-0012-1 postgresql postgresql-contrib postgresql-server
http://www.securityfocus.com/archive/1/archive/1/509917/100/0/threaded
* CONFIRM:
http://www.postgresql.org/docs/current/static/release-7-4-27.html
* CONFIRM:
http://www.postgresql.org/docs/current/static/release-8-0-23.html
* CONFIRM:
http://www.postgresql.org/docs/current/static/release-8-1-19.html
* CONFIRM:

http://www.postgresql.org/docs/current/static/release-8-2-15.html
* CONFIRM:
http://www.postgresql.org/docs/current/static/release-8-3-9.html
* CONFIRM:
http://www.postgresql.org/docs/current/static/release-8-4-2.html
* CONFIRM:
http://www.postgresql.org/support/security.html
* CONFIRM:
http://wiki.rpath.com/wiki/Advisories:rPSA-2010-0012
* FEDORA: FEDORA-2009-13363
https://www.redhat.com/archives/fedora-package-announce/2009-December/msg01035.html
* FEDORA: FEDORA-2009-13381
https://www.redhat.com/archives/fedora-package-announce/2009-December/msg01056.html
* MANDRIVA: MDVSA-2009:333
http://www.mandriva.com/security/advisories?name=MDVSA-2009:333
* SUSE: SUSE-SR:2010:001
http://lists.opensuse.org/opensuse-security-announce/2010-01/msg00007.html
* BID: 37334
http://www.securityfocus.com/bid/37334
* OSVDB: 61038
http://osvdb.org/61038
* SECTRACK: 1023325
http://www.securitytracker.com/id?1023325
* SECUNIA: 37663
http://secunia.com/advisories/37663
* VUPEN: ADV-2009-3519
http://www.vupen.com/english/advisories/2009/3519

CVE Reference:

CVE-2009-4034 (cve.mitre.org, nvd.nist.gov)

• 12175 PostgreSQL LDAP authentication with anonymous binds authentication bypass Vulnerability

The core server component in PostgreSQL 8.3 before 8.3.8 and 8.2 before 8.2.14, when using LDAP authentication with anonymous binds, allows remote attackers to bypass authentication via an empty password.

PostgreSQL versions prior to 8.2.14, and 8.3.8 are vulnerable to this issue.

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

References:

* BUGTRAQ: 20100307 rPSA-2010-0012-1 postgresql postgresql-contrib postgresql-server
http://www.securityfocus.com/archive/1/archive/1/509917/100/0/threaded
* CONFIRM:
http://www.postgresql.org/docs/8.3/static/release-8-3-8.html
* CONFIRM:
http://www.postgresql.org/support/security.html
* CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=522084
* CONFIRM:
http://wiki.rpath.com/wiki/Advisories:rPSA-2010-0012
* DEBIAN: DSA-1900
http://www.us.debian.org/security/2009/dsa-1900
* FEDORA: FEDORA-2009-9473
https://www.redhat.com/archives/fedora-package-announce/2009-September/msg00305.html
* FEDORA: FEDORA-2009-9474
https://www.redhat.com/archives/fedora-package-announce/2009-September/msg00307.html
* SUSE: SUSE-SR:2009:016
http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
* SUSE: SUSE-SR:2009:017
http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00004.html
* UBUNTU: USN-834-1
http://www.ubuntu.com/usn/usn-834-1
* BID: 36314
http://www.securityfocus.com/bid/36314
* SECUNIA: 36660
http://secunia.com/advisories/36660
* SECUNIA: 36727

http://secunia.com/advisories/36727
* SECUNIA: 36837
http://secunia.com/advisories/36837
* SECUNIA: 36800
http://secunia.com/advisories/36800

CVE Reference:

CVE-2009-3231 (cve.mitre.org, nvd.nist.gov)

• 12176 PostgreSQL RESET ROLE and RESET SESSION AUTHORIZATION Vulnerabilities

The core server component in PostgreSQL 8.4 before 8.4.1, 8.3 before 8.3.8, 8.2 before 8.2.14, 8.1 before 8.1.18, 8.0 before 8.0.22, and 7.4 before 7.4.26 does not use the appropriate privileges for the (1) RESET ROLE and (2) RESET SESSION AUTHORIZATION operations, which allows remote authenticated users to gain privileges. NOTE: this is due to an incomplete fix for CVE-2007-6600.

PostgreSQL versions prior to 7.4.26, 8.0.22, 8.1.18, 8.2.14, 8.3.8, and 8.4.1 are vulnerable to this issue.

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

References:

* BUGTRAQ: 20100307 rPSA-2010-0012-1 postgresql postgresql-contrib postgresql-server
http://www.securityfocus.com/archive/1/archive/1/509917/100/0/threaded
* MLIST: [pgsql-www] 20090909 Re: Incorrect CVE reference on security page
http://archives.postgresql.org/pgsql-www/2009-09/msg00024.php
* CONFIRM:
http://www.postgresql.org/docs/8.3/static/release-8-3-8.html
* CONFIRM:
http://www.postgresql.org/support/security.html
* CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=522085
* CONFIRM:
http://wiki.rpath.com/wiki/Advisories:rPSA-2010-0012
* DEBIAN: DSA-1900
http://www.us.debian.org/security/2009/dsa-1900
* FEDORA: FEDORA-2009-9473
https://www.redhat.com/archives/fedora-package-announce/2009-September/msg00305.html
* FEDORA: FEDORA-2009-9474
https://www.redhat.com/archives/fedora-package-announce/2009-September/msg00307.html
* SUNALERT: 270408
http://sunsolve.sun.com/search/document.do?assetkey=1-66-270408-1
* SUSE: SUSE-SR:2009:016
http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
* SUSE: SUSE-SR:2009:017
http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00004.html
* UBUNTU: USN-834-1
http://www.ubuntu.com/usn/usn-834-1
* BID: 36314
http://www.securityfocus.com/bid/36314
* SECUNIA: 36660
http://secunia.com/advisories/36660
* SECUNIA: 36695
http://secunia.com/advisories/36695
* SECUNIA: 36727
http://secunia.com/advisories/36727
* SECUNIA: 36837
http://secunia.com/advisories/36837
* SECUNIA: 36800
http://secunia.com/advisories/36800
* VUPEN: ADV-2009-2602
http://www.vupen.com/english/advisories/2009/2602

CVE Reference:

CVE-2009-3230 (cve.mitre.org, nvd.nist.gov)

• 12177 PostgreSQL "re-LOAD-ing" libraries Denial of Service Vulnerability

The core server component in PostgreSQL 8.4 before 8.4.1, 8.3 before 8.3.8, and 8.2 before 8.2.14 allows remote authenticated users to cause a denial of service (backend shutdown) by "re-LOAD-ing" libraries from a certain plugins directory.

PostgreSQL versions prior to 8.2.14, 8.3.8, and 8.4.1 are vulnerable to this issue.

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

References:

* BUGTRAQ: 20100307 rPSA-2010-0012-1 postgresql postgresql-contrib postgresql-server
http://www.securityfocus.com/archive/1/archive/1/509917/100/0/threaded
* CONFIRM:
http://www.postgresql.org/docs/8.3/static/release-8-3-8.html
* CONFIRM:
http://www.postgresql.org/support/security.html
* CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=522092
* CONFIRM:
http://wiki.rpath.com/wiki/Advisories:rPSA-2010-0012
* DEBIAN: DSA-1900
http://www.us.debian.org/security/2009/dsa-1900
* FEDORA: FEDORA-2009-9473
https://www.redhat.com/archives/fedora-package-announce/2009-September/msg00305.html
* FEDORA: FEDORA-2009-9474
https://www.redhat.com/archives/fedora-package-announce/2009-September/msg00307.html
* SUNALERT: 270408
http://sunsolve.sun.com/search/document.do?assetkey=1-66-270408-1
* SUSE: SUSE-SR:2009:016
http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
* SUSE: SUSE-SR:2009:017
http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00004.html
* UBUNTU: USN-834-1
http://www.ubuntu.com/usn/usn-834-1
* BID: 36314
http://www.securityfocus.com/bid/36314
* SECUNIA: 36660
http://secunia.com/advisories/36660
* SECUNIA: 36727
http://secunia.com/advisories/36727
* SECUNIA: 36837
http://secunia.com/advisories/36837
* SECUNIA: 36800
http://secunia.com/advisories/36800

CVE Reference:

CVE-2009-3229 (cve.mitre.org, nvd.nist.gov)

• 12178 PostgreSQL failure in the conversion of a localized error message Denial of Service Vulnerability

PostgreSQL before 8.3.7, 8.2.13, 8.1.17, 8.0.21, and 7.4.25 allows remote authenticated users to cause a denial of service (stack consumption and crash) by triggering a failure in the conversion of a localized error message to a client-specified encoding, as demonstrated using mismatched encoding conversion requests.

PostgreSQL versions prior to 7.4.25, 8.0.21, 8.1.17, 8.2.13, and 8.3.7 are vulnerable to this issue.

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

References:

* BUGTRAQ: 20090519 rPSA-2009-0086-1 postgresql postgresql-contrib postgresql-server
http://www.securityfocus.com/archive/1/archive/1/503598/100/0/threaded
* MLIST: [oss-security] 20090311 CVE request -- postgresql
http://www.openwall.com/lists/oss-security/2009/03/11/4
* MLIST: [pgsql-bugs] 20090227 BUG #4680: Server crashed if using wrong (mismatch) conversion functions
http://archives.postgresql.org/pgsql-bugs/2009-02/msg00172.php
* MLIST: [pgsql-bugs] 20090227 Re: BUG #4680: Server crashed if using wrong (mismatch) conversion functions
http://archives.postgresql.org//pgsql-bugs/2009-02/msg00176.php
* CONFIRM:
http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=517405
* CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=488156
* CONFIRM:

http://www.postgresql.org/about/news.1065
* CONFIRM:
http://wiki.rpath.com/Advisories:rPSA-2009-0086
* FEDORA: FEDORA-2009-2927
https://www.redhat.com/archives/fedora-package-announce/2009-March/msg00810.html
* FEDORA: FEDORA-2009-2959
https://www.redhat.com/archives/fedora-package-announce/2009-March/msg00843.html
* MANDRIVA: MDVSA-2009:079
http://www.mandriva.com/security/advisories?name=MDVSA-2009:079
* REDHAT: RHSA-2009:1067
http://www.redhat.com/support/errata/RHSA-2009-1067.html
* SUNALERT: 258808
http://sunsolve.sun.com/search/document.do?assetkey=1-66-258808-1
* SUNALERT: 1020455
http://sunsolve.sun.com/search/document.do?assetkey=1-77-1020455.1-1
* SUSE: SUSE-SR:2009:009
http://lists.opensuse.org/opensuse-security-announce/2009-04/msg00010.html
* BID: 34090
http://www.securityfocus.com/bid/34090
* SECTRACK: 1021860
http://www.securitytracker.com/id?1021860
* SECUNIA: 34453
http://secunia.com/advisories/34453
* SECUNIA: 35100
http://secunia.com/advisories/35100
* VUPEN: ADV-2009-0767
http://www.vupen.com/english/advisories/2009/0767
* VUPEN: ADV-2009-1316
http://www.vupen.com/english/advisories/2009/1316

CVE Reference:

CVE-2009-0922 (cve.mitre.org, nvd.nist.gov)

• 12179 PostgreSQL DBLink module privileges escalation Vulnerability

The DBLink module in PostgreSQL 8.2 before 8.2.6, 8.1 before 8.1.11, 8.0 before 8.0.15, 7.4 before 7.4.19, and 7.3 before 7.3.21, when local trust or ident authentication is used, allows remote attackers to gain privileges via unspecified vectors. NOTE: this issue exists because of an incomplete fix for CVE-2007-3278.

PostgreSQL versions prior to 7.4.25, 8.0.21, 8.1.17, 8.2.13, and 8.3.7 are vulnerable to this issue.

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

References:

* BUGTRAQ: 20080107 PostgreSQL 2007-01-07 Cumulative Security Release
http://www.securityfocus.com/archive/1/archive/1/485864/100/0/threaded
* BUGTRAQ: 20080115 rPSA-2008-0016-1 postgresql postgresql-server
http://www.securityfocus.com/archive/1/archive/1/486407/100/0/threaded
* CONFIRM:
http://www.postgresql.org/about/news.905
* CONFIRM:
https://issues.rpath.com/browse/RPL-1768
* DEBIAN: DSA-1460
http://www.debian.org/security/2008/dsa-1460
* DEBIAN: DSA-1463
http://www.debian.org/security/2008/dsa-1463
* FEDORA: FEDORA-2008-0478
https://www.redhat.com/archives/fedora-package-announce/2008-January/msg00397.html
* FEDORA: FEDORA-2008-0552
https://www.redhat.com/archives/fedora-package-announce/2008-January/msg00469.html
* GENTOO: GLSA-200801-15
http://security.gentoo.org/glsa/glsa-200801-15.xml
* HP: HPSBTU02325
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01420154
* MANDRIVA: MDVSA-2008:004
http://www.mandriva.com/security/advisories?name=MDVSA-2008:004
* REDHAT: RHSA-2008:0038
http://www.redhat.com/support/errata/RHSA-2008-0038.html
* REDHAT: RHSA-2008:0039

http://www.redhat.com/support/errata/RHSA-2008-0039.html
* REDHAT: RHSA-2008:0040
http://www.redhat.com/support/errata/RHSA-2008-0040.html
* SUNALERT: 103197
http://sunsolve.sun.com/search/document.do?assetkey=1-26-103197-1
* SUNALERT: 200559
http://sunsolve.sun.com/search/document.do?assetkey=1-66-200559-1
* SUSE: SUSE-SA:2008:005
http://lists.opensuse.org/opensuse-security-announce/2008-02/msg00000.html
* BID: 27163
http://www.securityfocus.com/bid/27163
* VUPEN: ADV-2008-0061
http://www.vupen.com/english/advisories/2008/0061
* VUPEN: ADV-2008-0109
http://www.vupen.com/english/advisories/2008/0109
* VUPEN: ADV-2008-1071
http://www.vupen.com/english/advisories/2008/1071/references
* SECTRACK: 1019157
http://securitytracker.com/id?1019157
* SECUNIA: 28359
http://secunia.com/advisories/28359
* SECUNIA: 28376
http://secunia.com/advisories/28376
* SECUNIA: 28438
http://secunia.com/advisories/28438
* SECUNIA: 28445
http://secunia.com/advisories/28445
* SECUNIA: 28437
http://secunia.com/advisories/28437
* SECUNIA: 28454
http://secunia.com/advisories/28454
* SECUNIA: 28464
http://secunia.com/advisories/28464
* SECUNIA: 28477
http://secunia.com/advisories/28477
* SECUNIA: 28479
http://secunia.com/advisories/28479
* SECUNIA: 28455
http://secunia.com/advisories/28455
* SECUNIA: 28679
http://secunia.com/advisories/28679
* SECUNIA: 28698
http://secunia.com/advisories/28698
* SECUNIA: 29638
http://secunia.com/advisories/29638
* XF: postgresql-dblink-privilege-escalation(39500)
http://xforce.iss.net/xforce/xfdb/39500

CVE Reference:

CVE-2007-6601 (cve.mitre.org, nvd.nist.gov)

• 14353 VNC is Running

In computing, Virtual Network Computing (VNC) is a graphical desktop sharing system that uses the RFB protocol to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction, over a network.

VNC (Virtual Network Computing) is running on the target.

As per PCI DSS v1.2 ASV Program guide 1.0:
â“Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix C or disabled/ removed. Please consult your ASV if you have questions about this Special Note.â”

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

References:

* MISC: Virtual Network Computing
http://en.wikipedia.org/wiki/Virtual_Network_Computing
* MISC:
http://www.realvnc.com/

CVE Reference:

• 14372 VNC Unauthenticated Access

In computing, Virtual Network Computing (VNC) is a graphical desktop sharing system that uses the RFB protocol to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction, over a network.

VNC (Virtual Network Computing) is running on the target and does not require authentication.

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

References:

* MISC: Virtual Network Computing
http://en.wikipedia.org/wiki/Virtual_Network_Computing
* MISC:
http://www.realvnc.com/

CVE Reference:

• 14381 VNC Security Type detection

In computing, Virtual Network Computing (VNC) is a graphical desktop sharing system that uses the RFB protocol to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction, over a network.

VNC (Virtual Network Computing) uses security types that might be more or less secure.

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

References:

* MISC: Virtual Network Computing
http://en.wikipedia.org/wiki/Virtual_Network_Computing
* MISC:
http://www.realvnc.com/

CVE Reference:

• 18815 VNC HTTP Server detection

In computing, Virtual Network Computing (VNC) is a graphical desktop sharing system that uses the RFB protocol to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction, over a network.

VNC HTTP Server (Virtual Network Computing) is running on the target.

As per PCI DSS v1.2 ASV Program guide 1.0:
â“Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix C or disabled/ removed. Please consult your ASV if you have questions about this Special Note.â”

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

References:

* MISC: Virtual Network Computing
http://en.wikipedia.org/wiki/Virtual_Network_Computing
* MISC:
http://www.realvnc.com/

CVE Reference:

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