netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 25

June 20, 2008

Table of Contents

Product Focus

CodeRed Worm Scanner – The S4 CodeRed Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any have been infected by CodeRed Worm.

CTO Jesper Jurcenoks of netVigilance is speaker at ITEC in Charlotte June 25, see **http://www.netvigilance.com/events**

This Week in Review

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

- **Gartner: iPhone 3G's business readiness still in question**

Businesses are eager to adopt the iPhone 3G but some questions about device security remain
It's been eight days since Apple officials publicly described new features and functions related to a July 11 release of its new iPhone 3G. However, prominent

industry analysts are saying that some of the basic information needed to judge its readiness for use in large companies, including details on security, is still unknown. Gartner analyst Ken Dulaney yesterday issued a near-glowing eight-page report on iPhone 3G as it relates to consumers. However, he said IT groups in large companies need to wait until second-generation software is available July 11 before they make a final decision on whether to support the iPhone.

infoworld

Full Story :
http://www.infoworld.com/article/08/06/17/Gartner_iPhone_3Gs_business_readiness_still_in_question_1.html?source=rss&url=http://www.infoworld.com/article/08/06/17/Gartner_iPhone_3Gs_business_readiness_still_in_question_1.html

❖ Mobile Data Matters

The plethora of technology devices we use in business today are adding to the risk of data loss for organisations of all shapes and sizes.

The mobile enterprise is beginning to become a reality - in 2009 IDC expects there to be 878 million mobile workers worldwide, which amounts to approximately 27% of the total workforce. Laptops and PDAs are commonplace across the corporate world, holding increasingly large amounts of valuable and, in many cases, confidential company data that could be easy prey for a new breed of criminals if left unprotected.

biosmagazine

Full Story :
http://www.biosmagazine.co.uk/op.php?id=907

❖ Compression technique lets attackers tap VoIP calls

New research suggests standard encryption and compression methods are not sufficiently secure and can make Internet telephone calls significantly more susceptible to bugging
A common compression technique can make Internet telephone calls significantly more susceptible to bugging, according to recent research from Johns Hopkins University. Internet telephony has become widely used through consumer-centric applications such as Skype, and is becoming more common in enterprises.

The new research suggests, however, that standard encryption and compression methods, when used together, are not sufficiently secure.

infoworld

Full Story :
http://www.infoworld.com/article/08/06/17/Compression_technique_lets_attackers_tap_VoIP_calls_1.html?source=rss&url=http://www.infoworld.com/article/08/06/17/Compression_technique_lets_attackers_tap_VoIP_calls_1.html

❖ Researchers urge ransomware victims to try file-recovery app

The security company that two weeks ago said it would lead a group effort to crack an encryption key used in a "ransomware" scam today offered victims more practical advice as it published instructions on how to recover data thought lost to the extortionists.

Moscow-based Kaspersky Lab added the instructions, which rely on an open-source file-recovery utility, to its writeup of Gpcode.ak, the Trojan horse that it first warned users about on June 8.

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=storage&articleId=9098338&taxonomyId=19&intsrc=kc_top

New Vulnerabilities Tested in SecureScout

- **15440 General Authentication - Accounts with No or Weak Passwords (Telnet) (1)**

Some Systems have been provided with Accounts with No or Weak Passwords. Such accounts MUST be disabled or passwords must be updated to avoid remote users to gain access to systems so easily. The level of privilege gained depends on the account used to access the system.

This TC will try the login/password combinations ranging from 1 to 10 in the dictionary files.

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

References:

* MISC: SANS Top 20 General UNIX Authentication Accounts with No Passwords or Weak Passwords

http://www.sans.org/top20/#U4

CVE Reference:

CVE-1999-0502 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0501 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0503 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0504 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0505 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0506 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0507 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0508 (cve.mitre.org, nvd.nist.gov)

- **15883 General Authentication - Accounts with No or Weak Passwords (Telnet) (2)**

Some Systems have been provided with Accounts with No or Weak Passwords. Such accounts MUST be disabled or passwords must be updated to avoid remote users to gain access to systems so easily. The level of privilege gained depends on the account used to access the system.

This TC will try the login/password combinations ranging from 11 to 20 in the dictionary files.

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

References:

* MISC: SANS Top 20 General UNIX Authentication Accounts with No Passwords or Weak Passwords

http://www.sans.org/top20/#U4

CVE Reference:

CVE-1999-0502 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0501 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0503 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0504 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0505 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0506 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0507 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0508 (cve.mitre.org, nvd.nist.gov)

- **16012 General Authentication - Accounts with No or Weak Passwords (Telnet) (3)**

Some Systems have been provided with Accounts with No or Weak Passwords. Such accounts MUST be disabled or passwords must be updated to avoid remote users to gain access to systems so easily. The level of privilege gained depends on the account used to access the system.

This TC will try the login/password combinations ranging from 21 to 30 in the dictionary files.

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

References:

* MISC: SANS Top 20 General UNIX Authentication Accounts with No Passwords or Weak Passwords

http://www.sans.org/top20/#U4

CVE Reference:

CVE-1999-0502 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0501 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0503 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0504 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0505 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0506 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0507 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0508 (cve.mitre.org, nvd.nist.gov)

- **16392 General Authentication - Accounts with No or Weak Passwords (Telnet) (4)**

Some Systems have been provided with Accounts with No or Weak Passwords. Such accounts MUST be disabled or passwords must be updated to avoid remote users to gain access to systems so easily. The level of privilege gained depends on the account used to access the system.

This TC will try the login/password combinations ranging from 31 to 40 in the dictionary files.

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

References:

* MISC: SANS Top 20 General UNIX Authentication Accounts with No Passwords or Weak Passwords

http://www.sans.org/top20/#U4

CVE Reference:

CVE-1999-0502 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0501 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0503 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0504 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0505 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0506 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0507 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0508 (cve.mitre.org, nvd.nist.gov)

• 16393 General Authentication - Accounts with No or Weak Passwords (Telnet) (5)

Some Systems have been provided with Accounts with No or Weak Passwords. Such accounts MUST be disabled or passwords must be updated to avoid remote users to gain access to systems so easily. The level of privilege gained depends on the account used to access the system.

This TC will try the login/password combinations ranging from 41 to 50 in the dictionary files.

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

References:

* MISC: SANS Top 20 General UNIX Authentication Accounts with No Passwords or Weak Passwords

http://www.sans.org/top20/#U4

CVE Reference:

CVE-1999-0502 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0501 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0503 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0504 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0505 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0506 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0507 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0508 (cve.mitre.org, nvd.nist.gov)

- **16394 General Authentication - Accounts with No or Weak Passwords (Telnet) (6)**

Some Systems have been provided with Accounts with No or Weak Passwords. Such accounts MUST be disabled or passwords must be updated to avoid remote users to gain access to systems so easily. The level of privilege gained depends on the account used to access the system.

This TC will try the login/password combinations ranging from 51 to 60 in the dictionary files.

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

References:

* MISC: SANS Top 20 General UNIX Authentication Accounts with No Passwords or Weak Passwords

http://www.sans.org/top20/#U4

CVE Reference:

CVE-1999-0502 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0501 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0503 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0504 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0505 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0506 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0507 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0508 (cve.mitre.org, nvd.nist.gov)

- **16488 General Authentication - Accounts with No or Weak Passwords (Telnet) (7)**

Some Systems have been provided with Accounts with No or Weak Passwords. Such accounts MUST be disabled or passwords must be updated to avoid remote users to gain access to systems so easily. The level of privilege gained depends on the account used to access the system.

This TC will try the login/password combinations ranging from 61 to 70 in the dictionary files.

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

References:

* MISC: SANS Top 20 General UNIX Authentication Accounts with No Passwords or Weak Passwords

http://www.sans.org/top20/#U4

CVE Reference:

CVE-1999-0502 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0501 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0503 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0504 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0505 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0506 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0507 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0508 (cve.mitre.org, nvd.nist.gov)

- **16955 General Authentication - Accounts with No or Weak Passwords (Telnet) (8)**

Some Systems have been provided with Accounts with No or Weak Passwords. Such accounts MUST be disabled or passwords must be updated to avoid remote users to

gain access to systems so easily. The level of privilege gained depends on the account used to access the system.

This TC will try the login/password combinations ranging from 71 to 80 in the dictionary files.

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

References:

* MISC: SANS Top 20 General UNIX Authentication Accounts with No Passwords or Weak Passwords

http://www.sans.org/top20/#U4

CVE Reference:

CVE-1999-0502 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0501 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0503 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0504 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0505 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0506 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0507 (cve.mitre.org, nvd.nist.gov)

CVE-1999-0508 (cve.mitre.org, nvd.nist.gov)

- **16956 QuickTime heap buffer overflow exists in handling of PixData structures when processing a PICT image (Remote File Checking)**

An issue in QuickTime's handling of PixData structures when processing a PICT image may result in a heap buffer overflow. Opening a maliciously crafted PICT image may lead to an unexpected application termination or arbitrary code execution. This issue does not affect systems running Mac OS X.

The issue has been fixed in version 7.5.0.

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

References:

* MISC:

http://secunia.com/secunia_research/2008-9/advisory/

* APPLE: APPLE-SA-2008-06-09

http://lists.apple.com/archives/security-announce/2008/Jun/msg00000.html

CVE Reference:

CVE-2008-1440 (cve.mitre.org, nvd.nist.gov)

- **16957 QuickTime memory corruption issue exists in handling of AAC-encoded media content (Remote File Checking)**

A memory corruption issue exists in QuickTime's handling of AAC-encoded media content. Opening a maliciously crafted media file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.5.0.

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

References:

* APPLE: APPLE-SA-2008-06-09

http://lists.apple.com/archives/security-announce/2008/Jun/msg00000.html

CVE Reference:

CVE-2008-1582 (cve.mitre.org, nvd.nist.gov)

- **16959 QuickTime stack buffer overflow exists in handling of Indeo video codec content (Remote File Checking)**

An issue in QuickTime's handling of Indeo video codec content may result in a stack buffer overflow. Viewing a maliciously crafted movie file with Indeo video codec content may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.5.0.

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

References:

* APPLE: APPLE-SA-2008-06-09

http://lists.apple.com/archives/security-announce/2008/Jun/msg00000.html

CVE Reference:

CVE-2008-1584 (cve.mitre.org, nvd.nist.gov)

- **16960 QuickTime URL handling issue exists in handling of "file:" URLs (Remote File Checking)**

A URL handling issue exists in QuickTime's handling of file: URLs. This may allow arbitrary applications and files to be launched when a user plays maliciously crafted QuickTime content in QuickTime Player.

The issue has been fixed in version 7.5.0.

The issue has been fixed in version 7.5.0.

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

References:

* APPLE: APPLE-SA-2008-06-09

http://lists.apple.com/archives/security-announce/2008/Jun/msg00000.html

CVE Reference:

CVE-2008-1585 (cve.mitre.org, nvd.nist.gov)

- **16961 QuickTime implementation issue allows untrusted Java applets to deserialize objects provided by QTJava (Remote File Checking)**

An implementation issue in QuickTime for Java allows untrusted Java applets to deserialize objects provided by QTJava. Visiting a web page containing a maliciously crafted Java applet could allow the disclosure of sensitive information, or arbitrary code execution with the privileges of the current user.

The issue has been fixed in version 7.4.5.

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

References:

* CONFIRM:

http://support.apple.com/kb/HT1241

* CERT: TA08-094A

http://www.us-cert.gov/cas/techalerts/TA08-094A.html

* BID: 28583

http://www.securityfocus.com/bid/28583

* FRSIRT: ADV-2008-1078

http://www.frsirt.com/english/advisories/2008/1078

* SECTRACK: 1019757

http://securitytracker.com/id?1019757

* SECUNIA: 29650

http://secunia.com/advisories/29650

* XF: quicktime-qtjava-code-execution(41601)

http://xforce.iss.net/xforce/xfdb/41601

CVE Reference:

CVE-2008-1013 (cve.mitre.org, nvd.nist.gov)

- **16962 QuickTime information disclosure when opening specially crafted QuickTime movies (Remote File Checking)**

Specially crafted QuickTime movies can automatically open external URLs, which may lead to information disclosure.

The issue has been fixed in version 7.4.5.

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

References:

* CONFIRM:

http://support.apple.com/kb/HT1241

* CERT: TA08-094A

http://www.us-cert.gov/cas/techalerts/TA08-094A.html

* BID: 28583

http://www.securityfocus.com/bid/28583

* FRSIRT: ADV-2008-1078

http://www.frsirt.com/english/advisories/2008/1078

* SECTRACK: 1019758

http://securitytracker.com/id?1019758

* SECUNIA: 29650

http://secunia.com/advisories/29650

* XF: quicktime-moviefiles-information-disclosure(41602)

http://xforce.iss.net/xforce/xfdb/41602

CVE Reference:

CVE-2008-1014 (cve.mitre.org, nvd.nist.gov)

- **16963 QuickTime handling of data reference atoms may result in a buffer overflow (Remote File Checking)**

An issue in QuickTime's handling of data reference atoms may result in a buffer overflow. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.4.5.

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

References:

* CONFIRM:

http://support.apple.com/kb/HT1241

* CERT: TA08-094A

http://www.us-cert.gov/cas/techalerts/TA08-094A.html

* BID: 28583

http://www.securityfocus.com/bid/28583

* FRSIRT: ADV-2008-1078

http://www.frsirt.com/english/advisories/2008/1078

* SECTRACK: 1019759

http://securitytracker.com/id?1019759

* SECUNIA: 29650

http://secunia.com/advisories/29650

* XF: quicktime-data-reference-bo(41604)

http://xforce.iss.net/xforce/xfdb/41604

CVE Reference:

CVE-2008-1015 (cve.mitre.org, nvd.nist.gov)

- **16964 QuickTime memory corruption issue exists in handling of movie media tracks (Remote File Checking)**

A memory corruption issue exists in QuickTime's handling of movie media tracks. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.4.5.

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

References:

* CONFIRM:

http://support.apple.com/kb/HT1241

* CERT: TA08-094A

http://www.us-cert.gov/cas/techalerts/TA08-094A.html

* BID: 28583

http://www.securityfocus.com/bid/28583

* FRSIRT: ADV-2008-1078

http://www.frsirt.com/english/advisories/2008/1078

* SECTRACK: 1019760

http://securitytracker.com/id?1019760

* SECUNIA: 29650

http://secunia.com/advisories/29650

* XF: quicktime-movie-media-code-execution(41605)

http://xforce.iss.net/xforce/xfdb/41605

CVE Reference:

CVE-2008-1016 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

Novell GroupWise Messenger (GWIM) Client, Multiple stack-based buffer overflows

"Execute arbitrary code"

Multiple stack-based buffer overflows in Novell GroupWise Messenger (GWIM) Client before 2.0.3 HP1 for Windows allow remote attackers to execute arbitrary code via "spoofed server responses."

References:
http://www.securityfocus.com/bid/29602

Novell iPrint Client ActiveX Control Parameter Handling Vulnerabilities

"Execution of arbitrary code"

Some vulnerabilities have been discovered in Novell iPrint Client, which can be exploited by malicious people to compromise a user's system.

The vulnerabilities are caused due to boundary errors in the included Novell iPrint ActiveX control (ienipp.ocx) when processing certain parameter values ("operation", "printer-url", and "target-frame"). These can be exploited to cause stack-based buffer overflows via overly long string values.

Successful exploitation allows execution of arbitrary code.

The vulnerabilities have been confirmed in version 4.34. Other versions may also be affected.

References:
http://support.novell.com/docs/Readmes/InfoDocument/patchbuilder/readme_5028061.html

Cisco VPN Client Deterministic Network Enhancer Privilege Escalation
"**Privilege Escalation**"

mu-b has reported a vulnerability in Cisco VPN Client, which can be exploited by malicious, local users to gain escalated privileges.

References:
http://www.digit-labs.org/files/exploits/dne2000-call.c

Vim Shell Command Injection Vulnerabilities
"Execute arbitrary commands"

Jan Minar has reported some vulnerabilities in Vim, which can be exploited by malicious people to compromise a user's system.

The vulnerabilities are caused due to the "filetype.vim", "tar.vim", "zip.vim", "xpm.vim", "xpm2.vim", "gzip.vim", and "netrw.vim" scripts improperly escaping special characters contained within filenames passed to the "execute" statement. This can be exploited to execute arbitrary commands on an affected system by tricking the user into opening specially crafted files.

The vulnerabilities are reported in versions 6.4 and 7.1.298. Other versions may also be affected.

References:
http://www.rdancer.org/vulnerablevim.html

Linux Kernel "pppol2tp_recvmsg()" Memory Corruption Vulnerability
"Denial of Service"

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

The vulnerability is caused due to a boundary error in the "pppol2tp_recvmsg()" function and can potentially be exploited to corrupt kernel memory via a specially crafted PPP over L2TP packet.

The vulnerability is reported in 2.6.x versions prior to 2.6.26-rc6.

References:
http://kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.26-rc6

Sun Solaris IP Multicast Filter Privilege Escalation
"Gain escalated privileges"

Tobias Klein has reported a vulnerability in Sun Solaris, which potentially can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to a signedness error in the IP kernel module when setting a socket's multi-cast filter. This can be exploited via a specially crafted "SIOCSIPMSFILTER" IOCTL requests.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-66-237965-1

Sun Solaris X Server Extensions Multiple Vulnerabilities
"Denial of Service; Disclose potentially sensitive information; Gain escalated privileges"

Sun has acknowledged multiple vulnerabilities in Solaris, which can be exploited by malicious, local users to cause a DoS (Denial of Service), disclose potentially sensitive information, or to gain escalated privileges.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-66-238686-1

Sun Solaris SNMPv3 Authentication Bypass
"Authentication bypass"

Sun has acknowledged a vulnerability in Solaris, which can be exploited by malicious people to spoof authenticated SNMPv3 packets.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-66-238865-1

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