netVigilance

ScoutNews Team **February 3, 2006**
2006 Issue # 5

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

OneCare has more than One hole, report on business cyber-crime, WinAmp zero-day exploit in the wild and AMD gets hacked in a major way.

Enjoy reading

Call or email netVigilance to get an update on SecureScout.
(503) 524 5758 or sales@netVigilance.com

Top Security News Stories this Week

- **Microsoft OneCare comes with holes**

The new service introduced by Microsoft with the intent of providing greater security for the average PC user, actually comes with some holes that could be exploited by an average hacker.

Apparently, any signed program or programs using JVM can bypass the security measures bundled in OneCare.

source

Full Story :
http://weblog.infoworld.com/securityadviser/archives/2006/01/microsofts_onec.html

- **Businesses get attacked more that previously thought**

The 1st Annual Enterprise Security Survey sheds light on the severity of cyber attacks toward businesses. The study also concluded that users are more interested in preventing attacks as opposed to detecting them. (Really! – *Ed.*)

ITObserver

Full Story :

http://www.ebcvg.com/articles.php?id=1054

- **WinAmp zero-day exploits emerge**

The popular music player software WinAmp contains a very serious vulnerability that can allow a hacker to gain complete control of an exploited PC.

The exploit takes advantage of the fact that WinAmp automatically begins playing a playlist once it's downloaded. Users can get infected simply by visiting a malicious site or by playing a infected playlist larger than about 1,040 bytes.

Information Week

Full Story :

http://www.informationweek.com/news/showArticle.jhtml?articleID=177105373

- **Hackers infect AMD support site**

Hackers exploiting a well publicized flaw in the way the Windows operating system render images that use the WMF (Windows Metafile) graphics format. Hackers discovered a way to deliver malicious wmf code to unsuspecting visitors to an AMD support site.

In a related story, the wmf exploit was first sold on a Russian hacker website back in December for $4,000.

InfoWorld

Related Links :

http://www.infoworld.com/article/06/01/30/74902_HNhackersamd_1.html
http://www.siliconvalleysleuth.com/2006/02/wmf_nightmare_s.html

New Vulnerabilities Tested in SecureScout

❖ 13333 Oracle Database Server - Net Listener component Unspecified error (jan-2006/DB09)

An unspecified error in the Net Listener component can potentially be exploited to gain knowledge of certain information, overwrite arbitrary files, and to conduct SQL injection attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html
http://www.red-database-security.com/advisory/oracle_tde_wallet_password.html
http://www.red-database-security.com/advisory/oracle_tde_unencrypted_sga.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft_int.html
http://www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
http://www.red-database-security.com/advisory/oracle_reports_read_any_xml_file.html
http://www.imperva.com/application_defense_center/papers/oracle-dbms-01172006.html

Other references:
http://secunia.com/advisories/16092/
http://www.kb.cert.org/vuls/id/150332
http://www.kb.cert.org/vuls/id/545804
http://www.kb.cert.org/vuls/id/870172
http://www.kb.cert.org/vuls/id/871756
http://www.kb.cert.org/vuls/id/891644
http://www.kb.cert.org/vuls/id/983340
http://www.kb.cert.org/vuls/id/999268

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

CVE Reference: None

❖ 13334 Oracle Database Server - Net Listener component Unspecified error (jan-2006/DB10)

An unspecified error in the Net Listener component can potentially be exploited to gain knowledge of certain information, overwrite arbitrary files, and to conduct SQL injection attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html

http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html
http://www.red-database-security.com/advisory/oracle_tde_wallet_password.html
http://www.red-database-security.com/advisory/oracle_tde_unencrypted_sga.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft_int.html
http://www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
http://www.red-database-security.com/advisory/oracle_reports_read_any_xml_file.html
http://www.imperva.com/application_defense_center/papers/oracle-dbms-01172006.html

Other references:
http://secunia.com/advisories/16092/
http://www.kb.cert.org/vuls/id/150332
http://www.kb.cert.org/vuls/id/545804
http://www.kb.cert.org/vuls/id/870172
http://www.kb.cert.org/vuls/id/871756
http://www.kb.cert.org/vuls/id/891644
http://www.kb.cert.org/vuls/id/983340
http://www.kb.cert.org/vuls/id/999268

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

CVE Reference: None

❖ 13335 Oracle Database Server - Net Listener component Unspecified error (jan-2006/DB11)

An unspecified error in the Net Listener component can potentially be exploited to gain knowledge of certain information, overwrite arbitrary files, and to conduct SQL injection attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html
http://www.red-database-security.com/advisory/oracle_tde_wallet_password.html
http://www.red-database-security.com/advisory/oracle_tde_unencrypted_sga.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft_int.html
http://www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
http://www.red-database-security.com/advisory/oracle_reports_read_any_xml_file.html
http://www.imperva.com/application_defense_center/papers/oracle-dbms-01172006.html

Other references:

http://secunia.com/advisories/16092/
http://www.kb.cert.org/vuls/id/150332
http://www.kb.cert.org/vuls/id/545804
http://www.kb.cert.org/vuls/id/870172
http://www.kb.cert.org/vuls/id/871756
http://www.kb.cert.org/vuls/id/891644
http://www.kb.cert.org/vuls/id/983340
http://www.kb.cert.org/vuls/id/999268

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

CVE Reference: None

❖ 13336 Oracle Database Server - Network Communications (RPC) component Unspecified error (jan-2006/DB12)

An unspecified error in the Network Communications (RPC) component can potentially be exploited to gain knowledge of certain information, overwrite arbitrary files, and to conduct SQL injection attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html
http://www.red-database-security.com/advisory/oracle_tde_wallet_password.html
http://www.red-database-security.com/advisory/oracle_tde_unencrypted_sga.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft_int.html
http://www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
http://www.red-database-security.com/advisory/oracle_reports_read_any_xml_file.html
http://www.imperva.com/application_defense_center/papers/oracle-dbms-01172006.html

Other references:
http://secunia.com/advisories/16092/
http://www.kb.cert.org/vuls/id/150332
http://www.kb.cert.org/vuls/id/545804
http://www.kb.cert.org/vuls/id/870172
http://www.kb.cert.org/vuls/id/871756
http://www.kb.cert.org/vuls/id/891644
http://www.kb.cert.org/vuls/id/983340
http://www.kb.cert.org/vuls/id/999268

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

CVE Reference: None

❖ 13337 Oracle Database Server - Network Communications (RPC) component Unspecified error (jan-2006/DB13)

An unspecified error in the Network Communications (RPC) component can potentially be exploited to gain knowledge of certain information, overwrite arbitrary files, and to conduct SQL injection attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html
http://www.red-database-security.com/advisory/oracle_tde_wallet_password.html
http://www.red-database-security.com/advisory/oracle_tde_unencrypted_sga.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft_int.html
http://www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
http://www.red-database-security.com/advisory/oracle_reports_read_any_xml_file.html
http://www.imperva.com/application_defense_center/papers/oracle-dbms-01172006.html

Other references:
http://secunia.com/advisories/16092/
http://www.kb.cert.org/vuls/id/150332
http://www.kb.cert.org/vuls/id/545804
http://www.kb.cert.org/vuls/id/870172
http://www.kb.cert.org/vuls/id/871756
http://www.kb.cert.org/vuls/id/891644
http://www.kb.cert.org/vuls/id/983340
http://www.kb.cert.org/vuls/id/999268

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

CVE Reference: None

❖ 13338 Oracle Database Server - Oracle Label Security component Unspecified error (jan-2006/DB14)

An unspecified error in the Oracle Label Security component can potentially be exploited to gain knowledge of certain information, overwrite arbitrary files, and to conduct SQL injection attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html
http://www.red-database-security.com/advisory/oracle_tde_wallet_password.html
http://www.red-database-security.com/advisory/oracle_tde_unencrypted_sga.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft_int.html
http://www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
http://www.red-database-security.com/advisory/oracle_reports_read_any_xml_file.html
http://www.imperva.com/application_defense_center/papers/oracle-dbms-01172006.html

Other references:
http://secunia.com/advisories/16092/
http://www.kb.cert.org/vuls/id/150332
http://www.kb.cert.org/vuls/id/545804
http://www.kb.cert.org/vuls/id/870172
http://www.kb.cert.org/vuls/id/871756
http://www.kb.cert.org/vuls/id/891644
http://www.kb.cert.org/vuls/id/983340
http://www.kb.cert.org/vuls/id/999268

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

CVE Reference: None

❖ 13339 Oracle Database Server - Oracle Text component Unspecified error (jan-2006/DB15)

An unspecified error in the Oracle Text component can potentially be exploited to gain knowledge of certain information, overwrite arbitrary files, and to conduct SQL injection attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html
http://www.red-database-security.com/advisory/oracle_tde_wallet_password.html
http://www.red-database-security.com/advisory/oracle_tde_unencrypted_sga.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft_int.html
http://www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
http://www.red-database-security.com/advisory/oracle_reports_read_any_xml_file.html
http://www.imperva.com/application_defense_center/papers/oracle-dbms-01172006.html

Other references:
http://secunia.com/advisories/16092/
http://www.kb.cert.org/vuls/id/150332
http://www.kb.cert.org/vuls/id/545804
http://www.kb.cert.org/vuls/id/870172
http://www.kb.cert.org/vuls/id/871756
http://www.kb.cert.org/vuls/id/891644
http://www.kb.cert.org/vuls/id/983340
http://www.kb.cert.org/vuls/id/999268

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

CVE Reference: None

❖ 13340 Oracle Database Server - Oracle Text component Unspecified error (jan-2006/DB16)

An unspecified error in the Oracle Text component can potentially be exploited to gain knowledge of certain information, overwrite arbitrary files, and to conduct SQL injection attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html
http://www.red-database-security.com/advisory/oracle_tde_wallet_password.html
http://www.red-database-security.com/advisory/oracle_tde_unencrypted_sga.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft_int.html
http://www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
http://www.red-database-security.com/advisory/oracle_reports_read_any_xml_file.html
http://www.imperva.com/application_defense_center/papers/oracle-dbms-01172006.html

Other references:
http://secunia.com/advisories/16092/
http://www.kb.cert.org/vuls/id/150332
http://www.kb.cert.org/vuls/id/545804
http://www.kb.cert.org/vuls/id/870172
http://www.kb.cert.org/vuls/id/871756
http://www.kb.cert.org/vuls/id/891644
http://www.kb.cert.org/vuls/id/983340
http://www.kb.cert.org/vuls/id/999268

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

CVE Reference: None

❖ 13341 Oracle Database Server - Oracle Text component Unspecified error (jan-2006/DB17)

An unspecified error in the Oracle Text component can potentially be exploited to gain knowledge of certain information, overwrite arbitrary files, and to conduct SQL injection attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html
http://www.red-database-security.com/advisory/oracle_tde_wallet_password.html
http://www.red-database-security.com/advisory/oracle_tde_unencrypted_sga.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft_int.html
http://www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
http://www.red-database-security.com/advisory/oracle_reports_read_any_xml_file.html
http://www.imperva.com/application_defense_center/papers/oracle-dbms-01172006.html

Other references:
http://secunia.com/advisories/16092/
http://www.kb.cert.org/vuls/id/150332
http://www.kb.cert.org/vuls/id/545804
http://www.kb.cert.org/vuls/id/870172
http://www.kb.cert.org/vuls/id/871756
http://www.kb.cert.org/vuls/id/891644
http://www.kb.cert.org/vuls/id/983340
http://www.kb.cert.org/vuls/id/999268

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

CVE Reference: None

❖ 13342 Oracle Database Server - Program Interface Network component Unspecified error (jan-2006/DB18)

An unspecified error in the Program Interface Network component can potentially be exploited to gain knowledge of certain information, overwrite arbitrary files, and to conduct SQL injection attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html
http://www.red-database-security.com/advisory/oracle_tde_wallet_password.html
http://www.red-database-security.com/advisory/oracle_tde_unencrypted_sga.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft.html
http://www.red-database-security.com/advisory/oracle_sql_injection_kupv$ft_int.html
http://www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
http://www.red-database-security.com/advisory/oracle_reports_read_any_xml_file.html
http://www.imperva.com/application_defense_center/papers/oracle-dbms-01172006.html

Other references:
http://secunia.com/advisories/16092/
http://www.kb.cert.org/vuls/id/150332
http://www.kb.cert.org/vuls/id/545804
http://www.kb.cert.org/vuls/id/870172
http://www.kb.cert.org/vuls/id/871756
http://www.kb.cert.org/vuls/id/891644
http://www.kb.cert.org/vuls/id/983340
http://www.kb.cert.org/vuls/id/999268

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

CVE Reference: None

New Vulnerabilities found this Week

Winamp Three Playlist Parsing Buffer Overflow Vulnerabilities
"Buffer overflow"

Some vulnerabilities have been reported in Winamp, which can be exploited by malicious people to compromise a user's system.

1) A boundary error during the handling of filenames including a UNC path with a long computer name can be exploited to cause a buffer overflow via a specially crafted playlist containing a filename with an overly long computer name (about 1040 bytes).

NOTE: An exploit is publicly available.

The vulnerability has been confirmed in version 5.12. Other versions may also be affected.

2) A boundary error within the parsing of playlists (.m3u or .pls) can be exploited to cause a stack-based buffer overflow via a playlist containing an overly long, specially crafted filename.

The vulnerability has been reported in version 5.11 and does reportedly not affect prior versions.

The vulnerability is related to vulnerability #1.

3) A boundary error within the parsing of playlists containing a filename with a .wma extension can be exploited to cause a buffer overflow via a specially crafted playlist.

The vulnerability has been reported in version 5.094. Other versions may also be affected.

Successful exploitation of any of the vulnerabilities allows execution of arbitrary code on a user's system when e.g. a malicious website is visited.

References:
http://milw0rm.com/id.php?id=1458
http://www.idefense.com/intelligence/vulnerabilities/display.php?id=377
http://www.idefense.com/intelligence/vulnerabilities/display.php?id=378
http://www.kb.cert.org/vuls/id/604745

Firefox Multiple Vulnerabilities
"Conduct cross-site scripting attacks; Disclose sensitive information"

Multiple vulnerabilities have been reported in Firefox, which can be exploited by malicious people to bypass certain security restrictions, conduct cross-site scripting attacks, potentially disclose sensitive information, and potentially compromise a user's system.

1) Some errors in the JavaScript engine where certain temporary variables are not properly protected may be exploited to execute arbitrary code via a user-defined method triggering garbage collection.

One of the vulnerabilities affects only version 1.5. The other affects version 1.5 and prior.

2) An error in the dynamic style handling can be exploited to reference freed memory by changing the style of an element from "position:relative" to "position:static".

Successful exploitation may allow execution of arbitrary code.

The vulnerability has been reported in version 1.5.

3) An error in the "QueryInterface" method of the Location and Navigator objects can be exploited to cause a memory corruption.

Successful exploitation may allow execution of arbitrary code.

The vulnerability has been reported in version 1.5.

4) An input validation error in the processing of the attribute name when calling "XULDocument.persist()" can be exploited to inject arbitrary XML and JavaScript code in "localstore.rdf", which will be executed with the permissions of the

browser the next time the browser starts up again.

5) Some integer overflows in the E4X, SVG, and Canvas functionalities may be exploited to execute arbitrary code.

The vulnerabilities have been reported in version 1.5.

6) A boundary error in the "nsExpatDriver::ParseBuffer()" function in the XML parser may be exploited to disclose data on the heap.

The vulnerability does not affect version 1.0.

7) The internal "AnyName" object of the E4X functionality is not properly protected. This can be exploited to create a communication channel between two windows or frames having different domains.

This does not pose any direct risks and does not allow bypass of same-origin restrictions or disclosure of web content from other domains.

The vulnerability does not affect version 1.0.

References:
http://www.mozilla.org/security/announce/mfsa2006-01.html
http://www.mozilla.org/security/announce/mfsa2006-02.html
http://www.mozilla.org/security/announce/mfsa2006-04.html
http://www.mozilla.org/security/announce/mfsa2006-05.html
http://www.mozilla.org/security/announce/mfsa2006-06.html
http://www.mozilla.org/security/announce/mfsa2006-07.html
http://www.mozilla.org/security/announce/mfsa2006-08.html

Cisco VPN 3000 Concentrator HTTP Packet Denial of Service
"Denial of Service"

Eldon Sprickerhoff has reported a vulnerability in Cisco VPN 3000 Concentrator, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error when processing HTTP packets. This can be exploited to cause the network device to halt and drop established user connections by sending about 40 specially crafted HTTP packet to the concentrator.

Successful exploitation requires that the HTTP service is enabled (default setting) and may disable the network device requiring a reboot the regain functionality.

According to the vendor, the vulnerability affects software versions 4.7.0 through 4.7.2.A (including version 4.7REL). The discoverer of the vulnerability also reports the vulnerability in version 4.7.2.B. Software versions prior to 4.7.x are not affected.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20060126-vpn.shtml
http://www.esentire.com/news/vuln-cisco-vpn.html

Mercury Mail Transport System Buffer Overflow

"Buffer overflow"

kcope has discovered a vulnerability in Mercury Mail Transport System, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the request handling in the "MercuryH PH Directory Server" protocol module. This can be exploited to cause a buffer overflow by sending overly long data to port 105/tcp.

Successful exploitation allows execution of arbitrary code.

NOTE: Exploit code is publicly available.

The vulnerability has been confirmed in version 4.01b, and reported in version 4.01a and all 4.10 beta versions. Prior versions may also be affected.

An unspecified possible vulnerability has also been reported by the vendor in the MercuryW PopPass server.

References:
http://www.pmail.com/newsflash.htm#whfix

FreeBSD "pf" IP Fragment Denial of Service Vulnerability
"Denial of Service"

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

The vulnerability is caused due to an error in the "pf" Internet Protocol packet-filter fragment cache when handling IP fragments. This can be exploited to crash the system by sending a specially-crafted sequence of IP packet fragments to the packet filter.

Successful exploitation requires that "pf" is used with a ruleset containing "scrub fragment crop" or "scrub fragment drop-ovl" rules.

The vulnerability has been reported in version 5.3, 5.4, and 6.0.

References:
ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-06:07.pf.asc

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