netVigilance

ScoutNews Team

March 31, 2006
2006 Issue # 13

Weekly ScoutNews by netVigilance

Table of Contents

Interop 2006 -

See netVigilance at Interop 2006. If you are planning on attending Interop 2006 in Las Vegas, May 1-4, stop by booth #1206 and take in the live hacker demo.

Product Focus – MyDoom worm scanner. Use this free SecureScout Single Scanner to search for MyDoom variants.

This Week in Review

BBC stories used by hackers in new disturbing type of attacks, nasty P2P Trojan uncovered, Former employees may be greatest hacker threat and '007' gets busted.

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

- **Hackers use BBC stories to plant Malware**

According to an alert issued by Websense Security Labs, excerpts from actual BBC News stories are being used to lure IE users to Web sites that launch drive-by downloads of bots, spyware, back doors and other Trojan download scripts.

Using legitimate BBC news articles, hackers imbed a 'Read More' link at the bottom of the excerpt which redirects to a spoofed BBC link. From here the unsuspecting user gets a keylogger program installed.

The spoofed site exploits the unpatched createTextRange vulnerability to install the malware without user interaction. This vulnerability can be negated by disabling Active Scripting in Internet Explorer.

Follow these steps to turn off Active Scripting in Microsoft Internet Explorer **5.0, 5.01, 5.5, 6**:

1. On the Internet Explorer menu bar, follow **Tools** -> **Internet Options**.
2. Click the **Security** tab.
3. Select **Internet** and then **Custom Level.**
4. Under the **Scripting** heading, **Settings** section, **Active Scripting and Scripting of Java applets,** click **Disable,** and then **OK.**
5. Click **Local intranet,** and then click **Custom Level.**
6. Under the **Scripting** heading, **Settings** section, **Active Scripting and Scripting of Java applets,** click **Disable,** and then **OK.**
7. Click **OK** to save changes.

To disable Active Scripting across an entire Active Directory/Domain using GPO, security administrators should reference the following Microsoft links:
Internet Explorer Administrator Kit
Group Policy Reference Guide

To disable active scripting in versions earlier than 5.0 see Microsoft tech. bulletin: http://support.microsoft.com/kb/q154036/.

❖ Microworld Technologies uncover P2P Trojan

Security Engineers from Microworld Technologies uncovered a new Trojan dubbed Trojan.Win32.Inject.t or W32/Inject-H that exploits weaknesses in Windows Peer-to-Peer (P2P) networking.

Inject.t runs in the background, working as a Server that allows a hacker to control the system via IRC channels.

ITObserver

Full Story :
http://www.ebcvg.com/news/5978/peer_to_peer_trojan_worm_attacks_enterprises/

- **Former employees pose greatest potential hacker damage.**

A survey jointly conducted by CERT and the U.S. Secret Service found that former and often disgruntled employees with IT knowledge, have the potential to do more harm that the 'run of the mill hacker'.

The survey shows that of the insiders who cause security breaches, 59 percent were former employees or former contractors. Of those, 48 percent had been fired, 38 percent had resigned and 7 percent had been laid off. Source
Datamation

Full Story :
http://itmanagement.earthweb.com/secu/article.php/3595456

- **Brits nab al-Qaeda '007' hacker**

After Scotland Yard arrested a 22-year-old West Londoner, Younis Tsouli, suspected of participating in an alleged bomb plot; the mysterious hacker known as "Irhabi -- Terrorist – 007" ended his 2-year spree of hacking systems as U.S. Universities, spewing jihadist propaganda and teaching his craft to other Islamic radicals.

Although 007 was shut down, his actions bode of other, more destructive terrorist hackers that will emerge.
Washington Post

Related Links :
http://stygius.typepad.com/stygius/2006/03/british_uncover.html

New Vulnerabilities Tested in SecureScout

- **14048 Samba Exposure of Machine Account Credentials Vulnerability**

A security issue has been reported in Samba, which can be exploited by malicious, local users to gain knowledge of sensitive information.

The winbindd daemon saves the machine trust account credentials to the world-readable winbind log files in clear text. This may expose the credentials, which can be used to impersonate the server in a domain and gain additional information.

Successful exploitation requires that log level is set to 5 or above.

The security issue has been reported in versions 3.0.21 through 3.0.21c.

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

References:

Initial advisory:
http://us1.samba.org/samba/security/CAN-2006-1059.html

Other references:
http://us1.samba.org/samba/ftp/patches/security/samba-3.0.21-CAN-2006-1059.patch

Product Page:
http://www.samba.org

CVE Reference: CVE-2006-1059

❖ 16181 PHP "html_entity_decode()" Information Disclosure Vulnerability

A vulnerability has been discovered in PHP, which can be exploited by malicious people to gain knowledge of potentially sensitive information.

The vulnerability is caused due to the "html_entity_decode()" PHP function not being binary safe. This can be exploited to disclose certain part of the memory via a script calling the "html_entity_decode()" function with input controlled by the attacker and where the result is sent to the attacker.

Successful may allow disclosure of e.g. passwords stored in a PHP script.

The vulnerability has been confirmed in versions 4.4.2 and 5.1.2. Prior versions may also be affected.

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

References:

Original Advisory:

http://archives.neohapsis.com/archives/fulldisclosure/2006-03/1675.html

Other references:

http://secunia.com/advisories/19383/

http://www.php.net/downloads.php

Product Page:

http://www.php.net/

CVE Reference: None

❖ 16182 PHP "mb_send_mail()" function bypassing restrictions Vulnerability

Cdric Clerget has discovered a vulnerability in PHP, which can be exploited by malicious people to bypass certain security restrictions.

The PHP "mb_send_mail()" function allows additional parameters to be passed to sendmail via the "additional_parameter" parameter. This can be exploited to cause sendmail to read arbitrary files on the system as configuration file and saving the resulting log file to arbitrary writable directories. The saved log file may contain portions of the file that was read as configuration file.

Example:
```
$additional_param = "-C ".$file_to_read." -X ".getcwd()."/".$output_file;
mb_send_mail($email_address, NULL, NULL, NULL, $additional_param);
```

Successful exploitation allows the bypassing of certain "safe_mode" and "open_basedir" restrictions.

The vulnerability has been confirmed in version 5.1.2 and also reported in version 4.x. Other versions may also be affected.

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

References:

Original Advisory:
* BUGTRAQ:20060228 (PHP) mb_send_mail security bypass
* URL:http://www.securityfocus.com/archive/1/archive/1/426342/100/0/threaded
* BUGTRAQ:20060301 Re: (PHP) mb_send_mail security bypass
* URL:http://www.securityfocus.com/archive/1/archive/1/426497/100/0/threaded

Other references:
* FRSIRT:ADV-2006-0772
* URL:http://www.frsirt.com/english/advisories/2006/0772
* OSVDB:23534
* URL:http://www.osvdb.org/23534
* SECUNIA:18694
* URL:http://secunia.com/advisories/18694

Product Page:
http://www.php.net/

CVE Reference: CVE-2006-1014, CVE-2006-1015

❖ 16183 PHP imap functions bypassing restrictions Vulnerability

Cdric Clerget has discovered a vulnerability in PHP, which can be exploited by malicious people to bypass certain security restrictions.

The PHP imap functions e.g. "imap_open()", "imap_body()", and "imap_list()" can be exploited to read arbitrary files and obtain listings of arbitrary directories even when "safe_mode" and "open_basedir" are configured. It is reportedly also possible to create, delete, and rename files with apache privileges using the "imap_createmailbox()", "imap_deletemailbox()", and "imap_renamemailbox()" functions.

Successful exploitation allows bypassing of certain "safe_mode" and "open_basedir" restrictions.

The vulnerability has been confirmed in PHP version 4.4.2 compiled with c_client 2004g. Other versions may also be affected.

The vulnerability has been confirmed in version 5.1.2 and also reported in version 4.x. Other versions may also be affected.

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

References:

Original Advisory:
* BUGTRAQ:20060228 (PHP) imap functions bypass safemode and open_basedir restrictions
* URL:http://www.securityfocus.com/archive/1/archive/1/426339/100/0/threaded

Other references:
* FRSIRT:ADV-2006-0772
* URL:http://www.frsirt.com/english/advisories/2006/0772
* SECUNIA:18694
* URL:http://secunia.com/advisories/18694
* XF:php-imap-restriction-bypass(24964)
* URL:http://xforce.iss.net/xforce/xfdb/24964

Product Page:
http://www.php.net/

CVE Reference: CVE-2006-1017

❖ 16184 PHP session ID arbitrary HTTP headers injection Vulnerability

A vulnerability has been reported in PHP, which can be exploited by malicious people to conduct HTTP response splitting attacks, potentially conduct cross-site scripting attacks, and potentially compromise a vulnerable system.

Input passed to the session ID in the session extension isn't properly sanitised before being returned to the user via a "Set-Cookie" HTTP header. This can be exploited to

inject arbitrary HTTP headers, which will be included in the response sent to the user.

The vulnerability has been reported in versions 5.x through 5.1.1.

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

References:

Original Advisory:
http://www.hardened-php.net/advisory_012006.112.html

Other references:
* BUGTRAQ:20060112 Advisory 01/2006: PHP ext/session HTTP Response Splitting Vulnerability
* CONFIRM:http://www.php.net/release_5_1_2.php
* GENTOO:GLSA-200603-22
* URL:http://www.gentoo.org/security/en/glsa/glsa-200603-22.xml
* MANDRIVA:MDKSA-2006:028
* URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:028
* UBUNTU:USN-261-1
* URL:http://www.ubuntulinux.org/support/documentation/usn/usn-261-1
* BID:16220
* URL:http://www.securityfocus.com/bid/16220
* FRSIRT:ADV-2006-0177
* URL:http://www.frsirt.com/english/advisories/2006/0177
* FRSIRT:ADV-2006-0369
* URL:http://www.frsirt.com/english/advisories/2006/0369
* SECTRACK:1015484
* URL:http://securitytracker.com/id?1015484
* SECUNIA:18431
* URL:http://secunia.com/advisories/18431
* SECUNIA:18697
* URL:http://secunia.com/advisories/18697
* SECUNIA:19179
* URL:http://secunia.com/advisories/19179
* SECUNIA:19355
* URL:http://secunia.com/advisories/19355
* XF:php-session-response-splitting(24094)
* URL:http://xforce.iss.net/xforce/xfdb/24094

Product Page:
http://www.php.net/

CVE Reference: CVE-2006-0207

❖ 16185 PHP mysqli extension format string error

A vulnerability has been reported in PHP, which can be exploited by malicious people to execute arbitrary code.

A format string error in the processing of error messages in the mysqli extension may be exploited to execute arbitrary code by causing an exception in an application where the error message can be controlled by the attacker (e.g. when connecting to a database server with a malicious, invalid hostname).

Successful exploitation requires that certain conditions are met.

The vulnerability has been reported in versions 5.1.x through 5.1.1.

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

References:

Original Advisory:
http://www.hardened-php.net/advisory_022006.113.html

Other references:
http://secunia.com/advisories/18431/
http://www.php.net/release_5_1_2.php

Product Page:
http://www.php.net/

CVE Reference: None

❖ 16186 PHP input not properly sanitized leading to execution of arbitrary HTML and script code

A vulnerability has been reported in PHP, which can be exploited by malicious people to execute arbitrary code.

Some unspecified input passed under certain error conditions isn't properly sanitised before being returned to the user. This may be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

The vulnerability has been reported in versions 5.1.x through 5.1.1.

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

References:

Original Advisory:
http://www.php.net/release_5_1_2.php

Other references:
* CONFIRM:http://www.php.net/release_5_1_2.php
* GENTOO:GLSA-200603-22
* URL:http://www.gentoo.org/security/en/glsa/glsa-200603-22.xml
* MANDRIVA:MDKSA-2006:028
* URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:028
* UBUNTU:USN-261-1
* URL:http://www.ubuntulinux.org/support/documentation/usn/usn-261-1
* BID:16803
* URL:http://www.securityfocus.com/bid/16803
* FRSIRT:ADV-2006-0177
* URL:http://www.frsirt.com/english/advisories/2006/0177
* FRSIRT:ADV-2006-0369

* URL:http://www.frsirt.com/english/advisories/2006/0369
* MISC:https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=178028
* SECUNIA:18431
* URL:http://secunia.com/advisories/18431
* SECUNIA:18697
* URL:http://secunia.com/advisories/18697
* SECUNIA:19179
* URL:http://secunia.com/advisories/19179
* SECUNIA:19355
* URL:http://secunia.com/advisories/19355

Product Page:
http://www.php.net/

CVE Reference: CVE-2006-0208

❖ 16187 PHP "mysql_connect" Buffer Overflow Vulnerability

mercenary has discovered a vulnerability in PHP, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the handling of the named pipe part of the "server" parameter passed to the "mysql_connect()" PHP function in the "HANDLE create_named_pipe()" function in "libmysql.c". This can be exploited to cause a stack-based buffer overflow via a PHP script calling "mysql_connect()" where the "server" parameter can be controlled by the attacker.

NOTE: Exploit code is publicly available.

The vulnerability has been confirmed in version 4.4.1 for Windows. Versions 4.3.10 and 4.4.0 for Windows are reportedly also affected. Other versions may also be affected.

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

References:

Original Advisory:
http://lists.grok.org.uk/pipermail/full-disclosure/2006-January/041013.html

Other references:
http://secunia.com/advisories/18275/

Product Page:
http://www.php.net/

CVE Reference: None

❖ 16188 PHP "mb_send_mail()" "To:" Header Injection Vulnerability

s.masugata has reported a vulnerability in PHP, which potentially can be exploited by malicious people to use it as an open mail relay.

The vulnerability is caused due to an input validation error in the "mb_send_mail()" function. This can be exploited to inject arbitrary headers in a mail sent via a script calling the "mb_send_mail()" function where the "To" parameter can be controlled by the attacker.

The issue has been fixed in PHP version 5.1.0

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

References:

Original Advisory:
http://bugs.php.net/bug.php?id=35307

Other references:
* CONFIRM:http://www.php.net/release_5_1_0.php
* MANDRIVA:MDKSA-2005:238
* URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:238
* SUSE:SUSE-SA:2005:069
* URL:http://www.securityfocus.com/archive/1/archive/1/419504/100/0/threaded
* UBUNTU:USN-232-1
* URL:http://www.ubuntulinux.org/usn/usn-232-1/document_view
* BID:15571
* URL:http://www.securityfocus.com/bid/15571
* SECTRACK:1015296
* URL:http://securitytracker.com/id?1015296
* SECUNIA:17763
* URL:http://secunia.com/advisories/17763
* SECUNIA:18054
* URL:http://secunia.com/advisories/18054
* SECUNIA:18198
* URL:http://secunia.com/advisories/18198
* XF:php-mbsendmail-header-injection(23270)
* URL:http://xforce.iss.net/xforce/xfdb/23270

Product Page:
http://www.php.net/

CVE Reference: CAN-2005-3883

❖ 16189 Linux Kernel IP ID Value Increment Weakness

Marco Ivaldi has reported a weakness in the Linux kernel, which can be exploited by malicious people to disclose certain system information and potentially to bypass certain security restrictions.

The weakness is caused due to an error within the "ip_push_pending_frames()" function when creating a packet in reply to a received SYN/ACK packet. This causes RST packets to be sent with a IP ID value that is incremented per packet. This can potentially be exploited to conduct idle scan attacks.

The weakness has been reported in the 2.4 and 2.6 kernel branches.

The issue is fixed in version 2.6.16.1.

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

References:

Original advisory:
* BUGTRAQ:20060314 Linux zero IP ID vulnerability?
* URL:http://www.securityfocus.com/archive/1/archive/1/427622/100/0/threaded

Other references:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.1
http://www.kernel.org/git/?p=linux/kernel/git/stable/linux-2.6.16.y.git;a=commit;h=6f78133bf7a06845afee5bcdff7c276bbceaaf55
* BUGTRAQ:20060315 Re: Linux zero IP ID vulnerability?
* URL:http://www.securityfocus.com/archive/1/archive/1/427753/100/0/threaded
* BUGTRAQ:20060316 Re: Linux zero IP ID vulnerability?
* URL:http://www.securityfocus.com/archive/1/archive/1/427893/100/0/threaded
* BID:17109
* URL:http://www.securityfocus.com/bid/17109

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2006-1242

New Vulnerabilities found this Week

Samba Exposure of Machine Account Credentials
"Gain knowledge of sensitive information"

A security issue has been reported in Samba, which can be exploited by malicious, local users to gain knowledge of sensitive information.

The winbindd daemon saves the machine trust account credentials to the world-readable winbind log files in clear text. This may expose the credentials, which can be used to impersonate the server in a domain and gain additional information.

Successful exploitation requires that log level is set to 5 or above.

The security issue has been reported in versions 3.0.21 through 3.0.21c.

References:
http://us1.samba.org/samba/security/CAN-2006-1059.html

McAfee VirusScan DUNZIP32.dll Buffer Overflow Vulnerability
"Buffer overflow"

A vulnerability has been discovered in mcafee virusscan, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in a 3rd-party compression library

(DUNZIP32.dll) when processing virus definition files. This can be exploited to cause a buffer overflow via a specially crafted definition file.

Successful exploitation requires that the user is e.g. tricked into updating the virus definition file from a malicious site.

The vulnerability has been reported in McAfee VirusScan version 10.0.21 included with McAfee SecurityCenter Agent version 6.0.0.16. Prior versions may also be affected.

References:
http://www.networksecurity.fi/advisories/mcafee-virusscan.html

Sun Cluster SunPlex Manager File Disclosure Vulnerability
"Gain knowledge of potentially sensitive information"

A vulnerability has been reported in Sun Cluster, which can be exploited by malicious, local users to gain knowledge of potentially sensitive information.

The vulnerability is caused due to an unspecified error in the SunPlex Manager GUI. This can be exploited by a user, who has been granted the "solaris.cluster.gui" authorization, to view files that are normally inaccessible to the user.

The vulnerability has been reported in Sun Cluster version 3.1 4/04 for Solaris 8 and 9.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102278-1

MPlayer AVI "indx" Chunk and ASF Handling Vulnerabilities
"Denial of Service"

xfocus has reported some vulnerabilities in MPlayer, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially to compromise a user's system.

The vulnerabilities are caused due to integer overflow errors in "libmpdemux/asfheader.c" within the handling of an ASF file, and in "libmpdemux/aviheader.c" when parsing the "indx" chunk in an AVI file. This can be exploited to cause heap-based buffer overflows via a malicious ASF file, or via a AVI file with specially-crafted "wLongsPerEntry" and "nEntriesInUse" values in the "indx" chunk.

The vulnerability affects version 1.0pre7try2. Other version may also be affected.

References:
http://lists.grok.org.uk/pipermail/full-disclosure/2006-March/044615.html

PHP "html_entity_decode()" Information Disclosure Vulnerability
"Gain knowledge of potentially sensitive information"

A vulnerability has been discovered in PHP, which can be exploited by malicious people to gain knowledge of potentially sensitive information.

The vulnerability is caused due to the "html_entity_decode()" PHP function not being binary safe. This can be exploited to disclose certain part of the memory via a script calling the "html_entity_decode()" function with input controlled by the attacker and where the result is sent to the attacker.

Successful may allow disclosure of e.g. passwords stored in a PHP script.

The vulnerability has been confirmed in versions 4.4.2 and 5.1.2. Prior versions may also be affected.

References:
http://archives.neohapsis.com/archives/fulldisclosure/2006-03/1675.html

Sun Solaris Process Environment Disclosure Security Issue
"Gain knowledge of potentially sensitive information"

A security issue has been reported in Solaris, which can be exploited by malicious, local users to gain knowledge of potentially sensitive information.

The security issue is caused due to the "/usr/ucb/ps" command revealing the environment variables and values of all processes to an unprivileged user when run with the "-e" option. This can potentially reveal certain information of processes that belong to the root user.

The security issue has been reported in Solaris 8 and 9 on both the x86 and SPARC platforms.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102215-1

Linux Kernel IP ID Value Increment Weakness
"Disclose certain system information; bypass certain security restrictions"

Marco Ivaldi has reported a weakness in the Linux kernel, which can be exploited by malicious people to disclose certain system information and potentially to bypass certain security restrictions.

The weakness is caused due to an error within the "ip_push_pending_frames()" function when creating a packet in reply to a received SYN/ACK packet. This causes RST packets to be sent with a IP ID value that is incremented per packet. This can potentially be exploited to conduct idle scan attacks.

The weakness has been reported in the 2.4 and 2.6 kernel branches.

References:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.1
http://www.kernel.org/git/?p=linux/kernel/git/stable/linux-2.6.16.y.git;a=commit;h=6f78133bf7a06845afee5bcdff7c276bbceaaf55

Veritas NetBackup Multiple Buffer Overflow Vulnerabilities
"Buffer overflows; execution of arbitrary code"

Multiple vulnerabilities have been reported in Veritas Netbackup, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerabilities are caused due to boundary errors within the volume manager (vmd) daemon, the NetBackup Catalog (bpdbm) daemon, and the NetBackup Sharepoint Services server (bpspsserver) daemon. These can be exploited to cause buffer overflows when processing incoming, specially crafted packets.

Successful exploitation allows execution of arbitrary code.

The vulnerabilities affect the following products:
* NetBackup Enterprise Server/NetBackup Server; Server and Clients 6.0 (all platforms)
* NetBackup Enterprise Server/NetBackup Server; Server and Clients 5.1 (all platforms)
* NetBackup Enterprise Server/NetBackup Server; Server and Clients 5.0 (all platforms)
* NetBackup DataCenter and BusinesServer; Server and Clients 4.5FP (all platforms)
* NetBackup DataCenter and BusinesServer; Server and Clients 4.5MP (all platforms)

References:
http://securityresponse.symantec.com/avcenter/security/Content/2006.03.27.html
http://support.veritas.com/docs/281521

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