

Table of Contents

[Product Focus](#)

[This Week in Review](#)

[Top Security News Stories this Week](#)

[New Vulnerabilities Tested in SecureScout](#)

[New Vulnerabilities found this Week](#)

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://www2.netvigilance.com/productdownloads?productname=apachechunkedvulnerabilityscanner>

This Week in Review

New copyright bill under criticism. It's hacking season. Be aware of security issues on your iphone, android. Citibank customer data breached.

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

• Protect IP copyright bill faces growing criticism

Technologists are warning that the practical effects of a controversial copyright bill backed by Hollywood will "weaken" Internet security and cause other harmful side effects.

As more Internet engineers, networking professionals, and security specialists have evaluated the so-called Protect IP Act that was introduced last month, concern is growing about how it will change the end-to-end nature of the Internet in ways that could do more harm than good. (See CNET's previous coverage.)

The Protect IP Act would give the U.S. Department of Justice the power to seek a court order against an allegedly infringing Web site, and then serve that order on search engines, certain Domain Name System (DNS) providers, and Internet advertising firms, who would be required to make the target Web site invisible. It's sponsored by Senate Judiciary Committee Chairman Patrick Leahy, a Vermont Democrat, and aims to target overseas Web sites. Cnet Security

Full Story :

• Attacks on Sony, others show it's open hacking season

There seems to be a groundswell of hacking activity recently. From the Epsilon breach that touched dozens of major U.S. companies and their millions of customers, and RSA replacing its customers' SecurID tokens after attacks on several defense contractors to Sony sites getting pummeled by hackers on a regular basis--all within the last few months.

What's going on?

"I truly don't think there's a higher instance of hacking right now. I think there's been a wave of media coverage," said Bruce Schneier, chief security technology officer of BT and one of the most respected security experts around. "We saw the same thing with shark attacks. It's not that there are more shark attacks. It's that they made the news when people started looking for them." Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20069995-245/attacks-on-sony-others-show-its-open-hacking-season/?part=rss&

• Many top iPhone, Android apps face security woes

Some of the most popular applications available for the iPhone and Android handsets suffer from serious security issues, a recent study from security firm ViaForensics has found.

According to the security firm's appWatchdog study, a slew of companies, including Foursquare, LinkedIn, Netflix, and Wordpress earned a "fail" rating on storing sensitive data securely. Netflix's Android application, for example, failed to "securely store passwords," ViaForensics said. Surprisingly, the iPhone version of the Netflix app earned the highest "pass" rating for securely storing passwords.

Netflix is taking the findings seriously. In a statement to CNET, a company spokesman said that "Netflix members' privacy and personal-information security are a top priority for Netflix." The spokesman said that the streaming company will be "making a change on the app" to improve its security. Cnet Security

Full Story :

http://news.cnet.com/8301-13506_3-20070282-17/many-top-iphone-android-apps-face-security-woes/?part=rss&subj=

• Citibank cyberattack affects 210,000 customers

Citibank, the nation's third largest bank, this week disclosed that hackers broke into its systems and gained access to the personal information of hundreds of thousands of customers, the latest incident in a string of cyberattacks affecting major corporations. Those behind the attack gained access to Citibank's online banking platform, Citi Account Online, and viewed customer account numbers and contact information, including email addresses, a Citibank spokesman said in a statement send to SCMagazineUS.com on Thursday.

Social Security numbers, birth dates, card expiration dates and card security code (CVV) were not compromised.

The intrusion affected about one percent of Citibank's North American customers, the company said in its statement. SC Magazine

Full Story :

http://www.scmagazineus.com/citibank-cyberattack-affects-210000-customers/article/204857/?utm_source=feedburn

New Vulnerabilities Tested in SecureScout

• 19354 Adobe Flash Player 'SWF' File Remote Memory Corruption Vulnerability (CVE-2011-0611) (Remote File Checking)

Adobe Flash Player before 10.2.154.27 on Windows, Mac OS X, Linux, and Solaris and 10.2.156.12 and earlier on Android; Adobe AIR before 2.6.19140; and Authplay.dll (aka AuthPlayLib.bundle) in Adobe Reader 9.x before 9.4.4 and 10.x through 10.0.1 on Windows, Adobe Reader 9.x before 9.4.4 and 10.x before 10.0.3 on Mac OS X, and Adobe Acrobat 9.x before 9.4.4 and 10.x before 10.0.3 on Windows and Mac OS X allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via crafted Flash content; as demonstrated by a Microsoft Office document with an embedded .swf file that has a size inconsistency in a "group of included constants," object type confusion, ActionScript that adds custom functions to prototypes, and Date objects; and as exploited in the wild in April 2011.

Adobe Flash Player version 10.2.159.1 resolves the issue.

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

References:

* EXPLOIT-DB: 17175

<http://www.exploit-db.com/exploits/17175>

* MISC:

<http://bugix-security.blogspot.com/2011/04/cve-2011-0611-adobe-flash-zero-day.html>

* MISC:

<http://secunia.com/blog/210/>

* MISC:

<http://blogs.technet.com/b/mmpc/archive/2011/04/12/analysis-of-the-cve-2011-0611-adobe-flash-player-vulnerability-explo>

* MISC:

<http://contagiodump.blogspot.com/2011/04/apr-8-cve-2011-0611-flash-player-zero.html>

* CONFIRM:

<http://www.adobe.com/support/security/advisories/apsa11-02.html>

* CONFIRM:

<http://googlechromereleases.blogspot.com/2011/04/stable-channel-update.html>

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb11-07.html>

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb11-08.html>

* REDHAT: RHSA-2011:0451

<http://www.redhat.com/support/errata/RHSA-2011-0451.html>

* SUSE: SUSE-SA:2011:018

<http://lists.opensuse.org/opensuse-security-announce/2011-04/msg00004.html>

* CERT-VN: VU#230057

<http://www.kb.cert.org/vuls/id/230057>

* BID: 47314

<http://www.securityfocus.com/bid/47314>

* SECTRACK: 1025324

<http://www.securitytracker.com/id?1025324>

* SECTRACK: 1025325

<http://www.securitytracker.com/id?1025325>

* SECUNIA: 44141

<http://secunia.com/advisories/44141>

* SECUNIA: 44149

<http://secunia.com/advisories/44149>

* SECUNIA: 44119

<http://secunia.com/advisories/44119>

* VUPEN: ADV-2011-0922

<http://www.vupen.com/english/advisories/2011/0922>

* VUPEN: ADV-2011-0923

<http://www.vupen.com/english/advisories/2011/0923>

* VUPEN: ADV-2011-0924

<http://www.vupen.com/english/advisories/2011/0924>

* XF: adobe-flash-swf-doc-ce(66681)

<http://xforce.iss.net/xforce/xfdb/66681>

CVE Reference:

CVE-2011-0611 (cve.mitre.org, nvd.nist.gov)

● 19355 Adobe Flash Player information disclosure Vulnerability (CVE-2011-0579) (Remote File Checking)

Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to obtain sensitive information via unspecified vectors.

Adobe Flash Player version 10.3.181.14 resolves the issue.

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

References:

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb11-12.html>

* BID: 47847

<http://www.securityfocus.com/bid/47847>

* SECTRACK: 1025533

<http://securitytracker.com/id/1025533>

CVE Reference:

CVE-2011-0579 (cve.mitre.org, nvd.nist.gov)

• **19356 Adobe Flash Player integer overflow Vulnerability (CVE-2011-0618) (Remote File Checking)**

Integer overflow in Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code via unspecified vectors.

Adobe Flash Player version 10.3.181.14 resolves the issue.

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

References:

- * BID: 47815
<http://www.securityfocus.com/bid/47815>
- * SECTRACK: 1025533
<http://securitytracker.com/id/1025533>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-12.html>

CVE Reference:

CVE-2011-0618 (cve.mitre.org, nvd.nist.gov)

• **19357 Adobe Flash Player memory corruption Vulnerability (CVE-2011-0619) (Remote File Checking)**

Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0620, CVE-2011-0621, and CVE-2011-0622.

Adobe Flash Player version 10.3.181.14 resolves the issue.

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

References:

- * BID: 47806
<http://www.securityfocus.com/bid/47806>
- * SECTRACK: 1025533
<http://securitytracker.com/id/1025533>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-12.html>

CVE Reference:

CVE-2011-0619 (cve.mitre.org, nvd.nist.gov)

• **19358 Adobe Flash Player memory corruption Vulnerability (CVE-2011-0620) (Remote File Checking)**

Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0619, CVE-2011-0621, and CVE-2011-0622.

Adobe Flash Player version 10.3.181.14 resolves the issue.

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

References:

- * BID: 47807
<http://www.securityfocus.com/bid/47807>
- * SECTRACK: 1025533
<http://securitytracker.com/id/1025533>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-12.html>

CVE Reference:

CVE-2011-0620 (cve.mitre.org, nvd.nist.gov)

• **19359 Adobe Flash Player memory corruption Vulnerability (CVE-2011-0621) (Remote File Checking)**

Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0619, CVE-2011-0620, and CVE-2011-0622.

Adobe Flash Player version 10.3.181.14 resolves the issue.

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

References:

- * BID: 47808
<http://www.securityfocus.com/bid/47808>
- * SECTRACK: 1025533
<http://securitytracker.com/id/1025533>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-12.html>

CVE Reference:

CVE-2011-0621 (cve.mitre.org, nvd.nist.gov)

• **19360 Adobe Flash Player memory corruption Vulnerability (CVE-2011-0622) (Remote File Checking)**

Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0619, CVE-2011-0620, and CVE-2011-0621.

Adobe Flash Player version 10.3.181.14 resolves the issue.

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

References:

- * BID: 47809
<http://www.securityfocus.com/bid/47809>
- * SECTRACK: 1025533
<http://securitytracker.com/id/1025533>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-12.html>

CVE Reference:

CVE-2011-0622 (cve.mitre.org, nvd.nist.gov)

• **19361 Adobe Flash Player bounds checking Vulnerability (CVE-2011-0623) (Remote File Checking)**

Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code via unspecified vectors, related to a "bounds checking" issue, a different vulnerability than CVE-2011-0624, CVE-2011-0625, and CVE-2011-0626.

Adobe Flash Player version 10.3.181.14 resolves the issue.

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

References:

- * BID: 47811
<http://www.securityfocus.com/bid/47811>
- * SECTRACK: 1025533
<http://securitytracker.com/id/1025533>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-12.html>

CVE Reference:

CVE-2011-0623 (cve.mitre.org, nvd.nist.gov)

• **19362 Adobe Flash Player bounds checking Vulnerability (CVE-2011-0624) (Remote File Checking)**

Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code via unspecified vectors, related to a "bounds checking" issue, a different vulnerability than CVE-2011-0623, CVE-2011-0625, and CVE-2011-0626.

Adobe Flash Player version 10.3.181.14 resolves the issue.

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

References:

- * BID: 47812
<http://www.securityfocus.com/bid/47812>
- * SECTRACK: 1025533
<http://securitytracker.com/id/1025533>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-12.html>

CVE Reference:

CVE-2011-0624 (cve.mitre.org, nvd.nist.gov)

• **19363 Adobe Flash Player bounds checking Vulnerability (CVE-2011-0625) (Remote File Checking)**

Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code via unspecified vectors, related to a "bounds checking" issue, a different vulnerability than CVE-2011-0623, CVE-2011-0624, and CVE-2011-0626.

Adobe Flash Player version 10.3.181.14 resolves the issue.

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

References:

- * BID: 47813
<http://www.securityfocus.com/bid/47813>
- * SECTRACK: 1025533
<http://securitytracker.com/id/1025533>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-12.html>

CVE Reference:

CVE-2011-0625 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2011-1752 Apache CVSS 2.0 Score = 5.0**

The mod_dav_svn module for the Apache HTTP Server, as distributed in Apache Subversion before 1.6.17, allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a request for a baselined WebDAV resource, as exploited in the wild in May 2011. Per: <http://cwe.mitre.org/data/definitions/476.html> 'CWE-476: NULL Pointer Dereference'

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

- CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=709111
- BID: <http://www.securityfocus.com/bid/48091>
- DEBIAN: <http://www.debian.org/security/2011/dsa-2251>
- CONFIRM: <http://svn.apache.org/repos/asf/subversion/tags/1.6.17/CHANGES>
- CONFIRM: <http://subversion.apache.org/security/CVE-2011-1752-advisory.txt>
- SECUNIA: <http://secunia.com/advisories/44681>
- SECUNIA: <http://secunia.com/advisories/44633>

CVE Reference: [CVE-2011-1752](http://cve.mitre.org/cve/2011/1752)

• **CVE-2011-1783 Apache CVSS 2.0 Score = 4.3**

The mod_dav_svn module for the Apache HTTP Server, as distributed in Apache Subversion 1.5.x and 1.6.x before 1.6.17, when the SVNPathAuthz short_circuit option is enabled, allows remote attackers to cause a denial of service (infinite loop and memory consumption) in opportunistic circumstances by requesting data.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=709112

BID: <http://www.securityfocus.com/bid/48091>

DEBIAN: <http://www.debian.org/security/2011/dsa-2251>

CONFIRM: <http://svn.apache.org/repos/asf/subversion/tags/1.6.17/CHANGES>

CONFIRM: <http://subversion.apache.org/security/CVE-2011-1783-advisory.txt>

SECUNIA: <http://secunia.com/advisories/44681>

SECUNIA: <http://secunia.com/advisories/44633>

CVE Reference: [CVE-2011-1783](#)

• **CVE-2011-1921 Apache CVSS 2.0 Score = 4.3**

The mod_dav_svn module for the Apache HTTP Server, as distributed in Apache Subversion 1.5.x and 1.6.x before 1.6.17, when the SVNPathAuthz short_circuit option is disabled, does not properly enforce permissions for files that had been publicly readable in the past, which allows remote attackers to obtain sensitive information via a replay REPORT operation.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=709114

BID: <http://www.securityfocus.com/bid/48091>

DEBIAN: <http://www.debian.org/security/2011/dsa-2251>

CONFIRM: <http://svn.apache.org/repos/asf/subversion/tags/1.6.17/CHANGES>

CONFIRM: <http://subversion.apache.org/security/CVE-2011-1921-advisory.txt>

SECUNIA: <http://secunia.com/advisories/44681>

SECUNIA: <http://secunia.com/advisories/44633>

CVE Reference: [CVE-2011-1921](#)

• **CVE-2011-2395 Cisco CVSS 2.0 Score = 5.0**

The Neighbor Discovery (ND) protocol implementation in Cisco IOS on unspecified switches allows remote attackers to bypass the Router Advertisement Guarding functionality via a fragmented IPv6 packet in which the Router Advertisement (RA) message is contained in the second fragment, as demonstrated by (1) a packet in which the first fragment contains a long Destination Options extension header or (2) a packet in which the first fragment contains an ICMPv6 Echo Request message.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

FULLDISC: <http://seclists.org/fulldisclosure/2011/May/446>

CVE Reference: [CVE-2011-2395](#)

• **CVE-2011-1711 Novell CVSS 2.0 Score = 5.5**

Unspecified vulnerability in the Mobility Pack 1.1.2 and earlier in Novell Data Synchronizer 1.0.x, and 1.1.x through 1.1.1 build 428, allows remote authenticated users to access the accounts of other users via unknown vectors.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

CONFIRM: <http://www.novell.com/support/viewContent.do?externalId=7008690>

XF: <http://xforce.iss.net/xforce/xfdb/67840>

BID: <http://www.securityfocus.com/bid/48117>

SECUNIA: <http://secunia.com/advisories/44864>

CVE Reference: [CVE-2011-1711](#)

• **CVE-2011-0082 Mozilla CVSS 2.0 Score = 4.3**

The X.509 certificate validation functionality in Mozilla Firefox 4.0.x through 4.0.1 does not properly implement single-session security exceptions, which might make it easier for user-assisted remote attackers to spoof an SSL server via an untrusted certificate that triggers potentially unwanted local caching of documents from that server.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=709165

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=660749

BID: <http://www.securityfocus.com/bid/48064>

MLIST: <http://openwall.com/lists/oss-security/2011/05/31/9>

MLIST: <http://openwall.com/lists/oss-security/2011/05/31/4>

MLIST: <http://openwall.com/lists/oss-security/2011/05/31/18>

MLIST: <http://openwall.com/lists/oss-security/2011/05/31/14>

CONFIRM: <http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=627552>

CVE Reference: [CVE-2011-0082](#)

• **CVE-2011-2107 Adobe CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 10.3.181.22 on Windows, Mac OS X, Linux, and Solaris, and 10.3.185.22 and earlier on Android, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, related to a "universal cross-site scripting vulnerability." Per: <http://www.adobe.com/support/security/bulletins/apsb11-13.html> 'This issue also affects the authplay.dll component that ships with Adobe Reader and Acrobat X (10.0.3) and earlier 10.x and 9.x versions of Adobe Reader and Acrobat for Windows and Macintosh operating systems.'

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

CONFIRM: <http://www.adobe.com/support/security/bulletins/apsb11-13.html>

CVE Reference: [CVE-2011-2107](#)

• **CVE-2011-1823 Google CVSS 2.0 Score = 7.2**

The vold volume manager daemon on Android 2.2.3 trusts messages that are received from a PF_NETLINK socket, which allows local users to execute arbitrary code and gain root privileges via a negative index that bypasses a maximum-only signed integer check in the DirectVolume::handlePartitionAdded method, which triggers memory corruption, as demonstrated by Gingerbreak.

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

References:

CONFIRM: <http://android.git.kernel.org/?p=platform/system/netd.git;a=commit;h=79b579c92afc08ab12c0a5788d61f2dd2934836f>

CONFIRM: <http://android.git.kernel.org/?p=platform/system/core.git;a=commit;h=b620a0b1c7ae486e979826200e8e441605b0a5d6>

MISC: <http://xorl.wordpress.com/2011/04/28/android-vold-mpartminors-signedness-issue/>

MISC: <http://www.androidpolice.com/2011/05/03/google-patches-gingerbreak-exploit-but-dont-worry-we-still-have-root-for-now/>

MISC: <http://forum.xda-developers.com/showthread.php?t=1044765>

MISC: <http://c-skills.blogspot.com/2011/04/yummy-yummy-gingerbreak.html>

MISC: <http://androidcommunity.com/gingerbreak-root-for-gingerbread-app-20110421/>

CONFIRM:

<http://android.git.kernel.org/?p=platform/system/vold.git;a=commit;h=c51920c82463b240e2be0430849837d6fdc5352e>

CVE Reference: [CVE-2011-1823](#)

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