

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

This Week in Review

DDoS attack against Credit Card providers. Fake receipts target Amazon retailers. SC Magazine webcast on PCI compliance. Botnet targeting credit card account holders.

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

• Pro-WikiLeaks hackers target MasterCard, PayPal

Story updated on Wednesday, Dec. 8 at 2:12 p.m. EST

A united band of WikiLeaks supporters have knocked offline a number of high-profile websites that have taken a stand against the whistleblower organization and its founder.

The "hacktivist" group Anonymous, best known for DDoS attacks against the Church of Scientology and anti-piracy sites, shifted its focus over the weekend to target anti-WikiLeaks' websites, such as MasterCard and PayPal, with punishing distributed denial-of-service attacks. SC Magazine

Full Story :

http://www.scmagazineus.com/pro-wikileaks-hackers-target-mastercard-paypal/article/192415/?utm_source=feedbur

• Cybercrooks create fake Amazon receipts

The bad guys have created yet another online scam, this one involving fake Amazon receipts.

Targeting Amazon and its retail partners, cybercriminals are using a phony Amazon receipt generator to print bogus receipts, and then are asking for refunds from the retailer, claiming that the items they ordered were never received.

Reportedly discovered by security vendor GFI Software, this scam comes at an especially bad time, as online retailers are dealing with the onslaught of the holiday season. Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-20025172-83.html?part=rss&subj=news&tag=2547-1_3-0-20

• Free webcast today on PCI compliance

SC Magazine is presenting a free webcast today at 2 p.m. EST, focused on achieving PCI compliance. The Payment Card Industry Data Security Standard (PCI DSS) is known as one of the most prescriptive compliance mandates in the security marketplace. Yet, it still proves confounding to many executive leaders. Questions still abound around the proper solutions to satisfy the requirements, the best strategies to focus on or the proper measures for newer IT technologies now being adopted by many organizations, such as cloud, virtualization and mobile devices.

In this webcast, we hear from a leading expert about some of the tactical and strategic steps one can consider to get PCI compliant and also keep critical data safe from cyberattacks.

Ward Spangenberg (left), director of security operations at Zynga, a provider of social media games, will touch on things he has learned in getting compliant with PCI, providing some anecdotes and advice. SC Magazine

Full Story :

http://www.scmagazineus.com/free-webcast-today-on-pci-compliance/article/192281/?utm_source=feedburner&utm

• Zeus botnet targeting Macy's, Nordstrom account holders

A new Zeus botnet is targeting the credit card accounts of several major U.S. retailers, including Macy's and Nordstrom, researchers at online banking security firm Trusteer have warned.

The attack, discovered this week and currently ongoing, uses social engineering to trick users into handing over their retail credit card information and other sensitive data, Amit Klein, CTO of Trusteer, told SCMagazineUS.com on Thursday.

"We used to see Zeus only attacking banks and financial institutions," Klein said. "What we are seeing now is diversification." SC Magazine

Full Story :

http://www.scmagazineus.com/zeus-botnet-targeting-macys-nordstrom-account-holders/article/192509/?utm_source

New Vulnerabilities Tested in SecureScout

• 11033 PPTP VPN detected

The remote host is running a PPTP VPN (Point-to-Point Tunneling Protocol) which allows remote users to connect to a private network.

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

References:

* MISC: Microsoft's PPTP Implementation
<http://www.schneier.com/pptp-faq.html>

CVE Reference:

• 12077 SSL Server certificate validity period

SSL is a network layer that allows privacy in communications. Servers supporting SSL should use valid certificates.

Informational testcase displaying validity periods of the ssl certificates used by the remote target.

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

References:

* MISC: About the risk of using invalid certificates:
http://www.rsasecurity.com/products/keon/datasheets/KWS_DS_0702.pdf

CVE Reference:

- **12097 SSL Server certificate expiring within 120 days**

SSL is a network layer that allows privacy in communications. Servers supporting SSL should use valid certificates.

Informational testcase warning about currently valid ssl certificates expiring within 120 days.

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

References:

* MISC: About the risk of using invalid certificates:

http://www.rsasecurity.com/products/keon/datasheets/KWS_DS_0702.pdf

CVE Reference:

- **19084 Mozilla Thunderbird - Cross-site information disclosure via modal calls (Remote File Checking)**

Security researcher Eduardo Vela Nava reported that if a web page opened a new window and used a javascript: URL to make a modal call, such as alert(), then subsequently navigated the page to a different domain, once the modal call returned the opener of the window could get access to objects in the navigated window. This is a violation of the same-origin policy and could be used by an attacker to steal information from another web site.

The issue has been fixed in Thunderbird 3.0.9 and 3.1.5.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2010/mfsa2010-69.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=576616

* MANDRIVA: MDVSA-2010:210

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:210>

* MANDRIVA: MDVSA-2010:211

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:211>

* REDHAT: RHSA-2010:0782

<http://www.redhat.com/support/errata/RHSA-2010-0782.html>

CVE Reference:

CVE-2010-3178 (cve.mitre.org, nvd.nist.gov)

- **19085 Mozilla Firefox - Dangling pointer vulnerability in LookupGetterOrSetter (Remote File Checking)**

Security researcher regenrecht reported via TippingPoint's Zero Day Initiative that when window.__lookupGetter__ is called with no arguments the code assumes the top JavaScript stack value is a property name. Since there were no arguments passed into the function, the top value could represent uninitialized memory or a pointer to a previously freed JavaScript object. Under such circumstances the value is passed to another subroutine which calls through the dangling pointer, potentially executing attacker-controlled memory.

The issue has been fixed in Firefox 3.6.11 and 3.5.14.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2010/mfsa2010-67.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=598669

* MANDRIVA: MDVSA-2010:210

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:210>

* MANDRIVA: MDVSA-2010:211

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:211>

* REDHAT: RHSA-2010:0782

<http://www.redhat.com/support/errata/RHSA-2010-0782.html>

* REDHAT: RHSA-2010:0861

<http://www.redhat.com/support/errata/RHSA-2010-0861.html>

* REDHAT: RHSA-2010:0896

<http://www.redhat.com/support/errata/RHSA-2010-0896.html>

* UBUNTU: USN-997-1

<http://www.ubuntu.com/usn/USN-997-1>

* UBUNTU: USN-998-1

<http://www.ubuntu.com/usn/USN-998-1>

CVE Reference:

CVE-2010-3183 (cve.mitre.org, nvd.nist.gov)

• 19086 Mozilla Thunderbird - Dangling pointer vulnerability in LookupGetterOrSetter (Remote File Checking)

Security researcher regenrecht reported via TippingPoint's Zero Day Initiative that when `window.__lookupGetter__` is called with no arguments the code assumes the top JavaScript stack value is a property name. Since there were no arguments passed into the function, the top value could represent uninitialized memory or a pointer to a previously freed JavaScript object. Under such circumstances the value is passed to another subroutine which calls through the dangling pointer, potentially executing attacker-controlled memory.

The issue has been fixed in Thunderbird 3.1.5 and 3.0.9.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2010/mfsa2010-67.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=598669

* MANDRIVA: MDVSA-2010:210

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:210>

* MANDRIVA: MDVSA-2010:211

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:211>

* REDHAT: RHSA-2010:0782

<http://www.redhat.com/support/errata/RHSA-2010-0782.html>

* REDHAT: RHSA-2010:0861

<http://www.redhat.com/support/errata/RHSA-2010-0861.html>

* REDHAT: RHSA-2010:0896

<http://www.redhat.com/support/errata/RHSA-2010-0896.html>

* UBUNTU: USN-997-1

<http://www.ubuntu.com/usn/USN-997-1>

* UBUNTU: USN-998-1

<http://www.ubuntu.com/usn/USN-998-1>

CVE Reference:

CVE-2010-3183 (cve.mitre.org, nvd.nist.gov)

• 19087 Mozilla Firefox - Use-after-free error in nsBarProp (Remote File Checking)

Security researcher Sergey Glazunov reported that it was possible to access the locationbar property of a window object after it had been closed. Since the closed window's memory could have been subsequently reused by the system it was possible that an attempt to access the locationbar property could result in the execution of attacker-controlled memory.

The issue has been fixed in Firefox 3.6.11 and 3.5.14.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2010/mfsa2010-66.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=588929

* MANDRIVA: MDVSA-2010:210

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:210>

* MANDRIVA: MDVSA-2010:211

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:211>

* REDHAT: RHSA-2010:0781

<http://www.redhat.com/support/errata/RHSA-2010-0781.html>

* REDHAT: RHSA-2010:0782

<http://www.redhat.com/support/errata/RHSA-2010-0782.html>

* REDHAT: RHSA-2010:0780
<http://www.redhat.com/support/errata/RHSA-2010-0780.html>
* REDHAT: RHSA-2010:0861
<http://www.redhat.com/support/errata/RHSA-2010-0861.html>
* REDHAT: RHSA-2010:0896
<http://www.redhat.com/support/errata/RHSA-2010-0896.html>
* UBUNTU: USN-997-1
<http://www.ubuntu.com/usn/USN-997-1>
* UBUNTU: USN-998-1
<http://www.ubuntu.com/usn/USN-998-1>

CVE Reference:

CVE-2010-3180 (cve.mitre.org, nvd.nist.gov)

• 19088 Mozilla Thunderbird - Use-after-free error in nsBarProp (Remote File Checking)

Security researcher Sergey Glazunov reported that it was possible to access the locationbar property of a window object after it had been closed. Since the closed window's memory could have been subsequently reused by the system it was possible that an attempt to access the locationbar property could result in the execution of attacker-controlled memory.

The issue has been fixed in Thunderbird 3.0.9 and 3.1.5.

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

References:

* CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-66.html>
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=588929
* MANDRIVA: MDVSA-2010:210
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:210>
* MANDRIVA: MDVSA-2010:211
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:211>
* REDHAT: RHSA-2010:0781
<http://www.redhat.com/support/errata/RHSA-2010-0781.html>
* REDHAT: RHSA-2010:0782
<http://www.redhat.com/support/errata/RHSA-2010-0782.html>
* REDHAT: RHSA-2010:0780
<http://www.redhat.com/support/errata/RHSA-2010-0780.html>
* REDHAT: RHSA-2010:0861
<http://www.redhat.com/support/errata/RHSA-2010-0861.html>
* REDHAT: RHSA-2010:0896
<http://www.redhat.com/support/errata/RHSA-2010-0896.html>
* UBUNTU: USN-997-1
<http://www.ubuntu.com/usn/USN-997-1>
* UBUNTU: USN-998-1
<http://www.ubuntu.com/usn/USN-998-1>

CVE Reference:

CVE-2010-3180 (cve.mitre.org, nvd.nist.gov)

• 19089 Mozilla Firefox - Buffer overflow and memory corruption using document.write (Remote File Checking)

Security researcher Alexander Miller reported that passing an excessively long string to document.write could cause text rendering routines to end up in an inconsistent state with sections of stack memory being overwritten with the string data. An attacker could use this flaw to crash a victim's browser and potentially run arbitrary code on their computer.

The issue has been fixed in Firefox 3.5.14 and 3.6.11.

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

References:

* CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-65.html>
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=583077

* MANDRIVA: MDVSA-2010:210
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:210>
* MANDRIVA: MDVSA-2010:211
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:211>
* REDHAT: RHSA-2010:0782
<http://www.redhat.com/support/errata/RHSA-2010-0782.html>
* REDHAT: RHSA-2010:0861
<http://www.redhat.com/support/errata/RHSA-2010-0861.html>
* REDHAT: RHSA-2010:0896
<http://www.redhat.com/support/errata/RHSA-2010-0896.html>
* UBUNTU: USN-997-1
<http://www.ubuntu.com/usn/USN-997-1>
* UBUNTU: USN-998-1
<http://www.ubuntu.com/usn/USN-998-1>

CVE Reference:

CVE-2010-3179 (cve.mitre.org, nvd.nist.gov)

• 19090 Mozilla Thunderbird - Buffer overflow and memory corruption using document.write (Remote File Checking)

Security researcher Alexander Miller reported that passing an excessively long string to document.write could cause text rendering routines to end up in an inconsistent state with sections of stack memory being overwritten with the string data. An attacker could use this flaw to crash a victim's browser and potentially run arbitrary code on their computer.

The issue has been fixed in Thunderbird 3.0.9 and 3.1.5.

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

References:

* CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-65.html>
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=583077
* MANDRIVA: MDVSA-2010:210
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:210>
* MANDRIVA: MDVSA-2010:211
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:211>
* REDHAT: RHSA-2010:0782
<http://www.redhat.com/support/errata/RHSA-2010-0782.html>
* REDHAT: RHSA-2010:0861
<http://www.redhat.com/support/errata/RHSA-2010-0861.html>
* REDHAT: RHSA-2010:0896
<http://www.redhat.com/support/errata/RHSA-2010-0896.html>
* UBUNTU: USN-997-1
<http://www.ubuntu.com/usn/USN-997-1>
* UBUNTU: USN-998-1
<http://www.ubuntu.com/usn/USN-998-1>

CVE Reference:

CVE-2010-3179 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-4398 Microsoft CVSS 2.0 Score = 7.2

Stack-based buffer overflow in the RtlQueryRegistryValues function in win32k.sys in Microsoft Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008 through R2, and Windows 7 allows local users to gain privileges, and bypass the User Account Control (UAC) feature, via a crafted REG_BINARY value for a SystemDefaultEUDCFont registry key.

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

References:

CERT-VN: <http://www.kb.cert.org/vuls/id/529673>

EXPLOIT-DB: <http://www.exploit-db.com/exploits/15609/>

MISC: <http://www.exploit-db.com/bypassing-uac-with-user-privilege-under-windows-vista7-mirror/>

MISC: <http://twitter.com/msftsecresponse/statuses/7590788200402945>

SECUNIA: <http://secunia.com/advisories/42356>

MISC: <http://nakedsecurity.sophos.com/2010/11/25/new-windows-zero-day-flaw-bypasses-uac/>

MISC: <http://isc.sans.edu/diary.html?storyid=9988>

CVE Reference: [CVE-2010-4398](#)

• **CVE-2010-4408 Apache CVSS 2.0 Score = 6.8**

Apache Archiva 1.0 through 1.0.3, 1.1 through 1.1.4, 1.2 through 1.2.2, and 1.3 through 1.3.1 does not require entry of the administrator's password at the time of modifying a user account, which makes it easier for context-dependent attackers to gain privileges by leveraging a (1) unattended workstation or (2) cross-site request forgery (CSRF) vulnerability, a related issue to CVE-2010-3449.

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

References:

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/514937/100/0/threaded>

MLIST:

http://mail-archives.apache.org/mod_mbox/archiva-users/201011.mbox/ajax/%3CAANLkTimXeJHAuXdoUKLN=GkNty1_X

CONFIRM: <http://archiva.apache.org/security.html>

CVE Reference: [CVE-2010-4408](#)

• **CVE-2010-4108 HP CVSS 2.0 Score = 6.8**

HP HP-UX B.11.11, B.11.23, and B.11.31 does not properly support threaded processes, which allows remote authenticated users to cause a denial of service via unspecified vectors.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/3130>

BID: <http://www.securityfocus.com/bid/45219>

SECUNIA: <http://secunia.com/advisories/42499>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02586517>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02586517>

CVE Reference: [CVE-2010-4108](#)

• **CVE-2010-4109 HP CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in the Contacts Application in HP Palm webOS before 2.0 allows remote attackers to inject arbitrary web script or HTML via a crafted vCard file.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/3131>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02639302>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02639302>

CVE Reference: [CVE-2010-4109](#)

• **CVE-2010-2639 IBM CVSS 2.0 Score = 5.0**

IBM WebSphere Commerce Enterprise 7.0 before 7.0.0.2 allows remote attackers to read messages intended for other recipients via vectors involving access by the outbound messaging system to the RunTimeProfileCacheCmdImpl class, related to the caching of mutable objects and "concurrency issues."

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/63406>

AIXAPAR: <http://www-1.ibm.com/support/docview.wss?uid=swg1JR38114>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg24028397>

CVE Reference: [CVE-2010-2639](#)

• **CVE-2010-4409 PHP CVSS 2.0 Score = 5.0**

Integer overflow in the NumberFormatter::getSymbol (aka numfmt_get_symbol) function in PHP 5.3.3 and earlier allows context-dependent attackers to cause a denial of service (application crash) via an invalid argument.

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

References:

CERT-VN: <http://www.kb.cert.org/vuls/id/479900>

CONFIRM: <http://svn.php.net/viewvc?view=revision&revision=305571>

CONFIRM: http://svn.php.net/viewvc/php/php-src/trunk/ext/intl/formatter/formatter_attr.c?r1=305571&r2=305570&pathrev=305571

CVE Reference: [CVE-2010-4409](#)

• **CVE-2010-4254 Novell CVSS 2.0 Score = 7.5**

Mono, when Moonlight before 2.3.0.1 or 2.99.x before 2.99.0.10 is used, does not properly validate arguments to generic methods, which allows remote attackers to bypass generic constraints, and possibly execute arbitrary code, via a crafted method call.

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

References:

CONFIRM: <https://github.com/mono/mono/commit/cf1ec146f7c6acdc6697032b3aaafc68ffacdcac>

CONFIRM: <https://github.com/mono/mono/commit/65292a69c837b8a5f7a392d34db63de592153358>

CONFIRM: <https://github.com/mono/mono/commit/4905ef1130feb26c3150b28b97e4a96752e0d399>

CONFIRM: https://bugzilla.novell.com/show_bug.cgi?id=655847

CONFIRM: https://bugzilla.novell.com/show_bug.cgi?id=654136

CONFIRM: http://www.mono-project.com/Vulnerabilities#Moonlight_Generic_Constraints_Bypass_Vulnerability

SECUNIA: <http://secunia.com/advisories/42373>

CVE Reference: [CVE-2010-4254](#)

• **CVE-2010-4478 OpenSSH CVSS 2.0 Score = 7.5**

OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol, a related issue to CVE-2010-4252.

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

References:

MISC: <https://github.com/seb-m/jpake>

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=659297

CONFIRM: <http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/jpake.c.diff?r1=1.4;r2=1.5;f=h>

CONFIRM: <http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/jpake.c#rev1.5>

MISC: <http://seb.dbzteam.org/crypto/jpake-session-key-retrieval.pdf>

CVE Reference: [CVE-2010-4478](#)

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