

## 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

The team behind SecureScout has once again submitted a series of patches to the well known security tool Nmap; and as always the patches were approved immediately. These patches relate to fixing inconsistencies in the Nmap OS fingerprint database file. Nmap is massively used in the security industry especially by pen-testers, vulnerability assessment products, and hackers. Nmap was featured in the movie "Matrix Reloaded".

RSA conference on Cloud security. Survey shows IT security people having low security awareness. 2010 fraud incidents at higher costs. Activists hack security firm for revenge.

Enjoy reading & Stay safe.

**Call or email netVigilance to get an update on SecureScout.**

**(503) 524 5758 or [sales@netvigilance.com](mailto:sales@netvigilance.com)**

## Top Security News Stories this Week

### • RSA 2011: Cloud security challenges dominate

CSO - Security in the cloud is a hot topic, so it's no surprise that RSA Conference 2011 in San Francisco Feb. 14-18 will feature a number of sessions devoted to the issue.

In one session, "Cloud Computing Privacy and Security: The Legal, Ethical, Regulatory Framework," participants will discuss the various legal, ethical and regulatory issues in play and how organizations can address them effectively.

More on cloud computing and security Computerworld

Full Story :

### • Low security awareness found across IT

Computerworld - A broad spectrum of IT people, including those close to security functions, appear to have little awareness of key security issues impacting their organizations, a new survey shows.

The survey, which polled 430 members of the Oracle Application Users Group (OAUG) conducted by Unisphere Research and sponsored by Application Security Inc. included directors and managers of information technology, developers and programmers, database and systems administrators, systems architects and analysts and professionals from the HR and financial functions.

About 22% of respondents claimed to be extensively involved in security functions, 60% claimed a limited or supporting role, and the rest said they were not involved with security at all. About 100 respondents belonged to companies with more than 10,000 employees. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9208890/Low\\_security\\_awareness\\_found\\_across\\_IT\\_?source=rss\\_security](http://www.computerworld.com/s/article/9208890/Low_security_awareness_found_across_IT_?source=rss_security)

### • ID fraud incidents decline in 2010, but costs go up

Incidents of identity fraud declined last year, but the cost per incident rose, and consumers are taking longer to respond to occurrences of theft, according to a survey released Tuesday by Javelin Strategy & Research.

The eighth annual "2011 Identity Fraud Survey Report," which polled 5,000 U.S. adults, concluded, that the number of identity fraud incidents decreased 28 percent in 2010. Overall, 8.1 million U.S. adults fell victim to identity fraud in 2010, down from 11.1 million in 2009, according to the report.

The decrease may be attributed to a decline in the number of reported data breach incidents in 2010, according to the study. Seven percent of respondents said they were notified of a breach last year, down from 11 percent who were notified in 2009. SC Magazine

Full Story :

[http://www.scmagazineus.com/id-fraud-incidents-decline-in-2010-but-costs-go-up/article/195924/?utm\\_source=feed](http://www.scmagazineus.com/id-fraud-incidents-decline-in-2010-but-costs-go-up/article/195924/?utm_source=feed)

### • Anonymous takes over security firm in vengeful hack

HBGary has "completely unplugged from the internet" as the security firm moves into investigatory and damage control mode following the infiltration of its network over the weekend to steal some 50,000 corporate emails and credentials.

The hacker group Anonymous took responsibility for the hijack, apparently orchestrated out of revenge for plans by Aaron Barr, CEO of HBGary Federal, a sister firm to HBGary, to release information about the activist collective during a talk about social networking at the upcoming Security B-Sides show in San Francisco.

The group compromised a web server belonging to HBGary Federal, possibly exploiting an SQL vulnerability, to gain access to the network and discover the credentials for the company's Google email account, for which Barr was the administrator, HBGary CEO Greg Hoglund told SCMagazineUS.com on Monday. SC Magazine

Full Story :

[http://www.scmagazineus.com/anonymous-takes-over-security-firm-in-vengeful-hack/article/195837/?utm\\_source=feed](http://www.scmagazineus.com/anonymous-takes-over-security-firm-in-vengeful-hack/article/195837/?utm_source=feed)

## New Vulnerabilities Tested in SecureScout

### • 19187 PHP Apache 2 Local Denial of Service Vulnerability

The apache2handler SAPI (sapi\_apache2.c) in the Apache module (mod\_php) for PHP 5.x before 5.1.0 final and 4.4 before 4.4.1 final allows attackers to cause a denial of service (segmentation fault) via the session.save\_path option in a .htaccess file or VirtualHost.

The vulnerability has been reported in versions 4.4.0 and 5.0.5, and prior.

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

#### References:

- \* BUGTRAQ: 20051024 php &lt; 4.4.1 htaccess apache dos  
<http://marc.theaimsgroup.com/?l=bugtraq&am=113019286208204&w=2>
- \* FULLDISC: 20051024 php &lt; 4.4.1 htaccess apache dos  
<http://archives.neohapsis.com/archives/fulldisclosure/2005-10/0491.html>

\* CONFIRM:  
[http://bugs.gentoo.org/show\\_bug.cgi?id=107602](http://bugs.gentoo.org/show_bug.cgi?id=107602)

\* CONFIRM:  
<http://docs.info.apple.com/article.html?artnum=303382>

\* APPLE: APPLE-SA-2006-03-01  
<http://lists.apple.com/archives/security-announce/2006/Mar/msg00000.html>

\* GENTOO: GLSA-200511-08  
<http://www.gentoo.org/security/en/glsa/glsa-200511-08.xml>

\* HP: HPSBMA02159  
<http://itrc.hp.com/service/cki/docDisplay.do?docId=c00786522>

\* MANDRIVA: MDKSA-2005:213  
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:213>

\* CERT: TA06-062A  
<http://www.us-cert.gov/cas/techalerts/TA06-062A.html>

\* BID: 15177  
<http://www.securityfocus.com/bid/15177>

\* BID: 16907  
<http://www.securityfocus.com/bid/16907>

\* VUPEN: ADV-2006-0791  
<http://www.vupen.com/english/advisories/2006/0791>

\* VUPEN: ADV-2006-4320  
<http://www.vupen.com/english/advisories/2006/4320>

\* OSVDB: 20491  
<http://www.osvdb.org/20491>

\* SECUNIA: 18198  
<http://secunia.com/advisories/18198>

\* SECUNIA: 19064  
<http://secunia.com/advisories/19064>

\* SECUNIA: 17510  
<http://secunia.com/advisories/17510>

\* SECUNIA: 17557  
<http://secunia.com/advisories/17557>

\* SECUNIA: 22691  
<http://secunia.com/advisories/22691>

\* SREASON: 525  
<http://securityreason.com/securityalert/525>

\* XF: php-htaccess-dos(22844)  
<http://xforce.iss.net/xforce/xfdb/22844>

#### CVE Reference:

CVE-2005-3319 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19188 CSS Memory Corruption Vulnerability (MS11-003/2482017) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer accesses memory while importing a Cascading Style Sheet that refers to itself recursively. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

#### References:

\* EXPLOIT-DB: 15708  
<http://www.exploit-db.com/exploits/15708>

\* EXPLOIT-DB: 15746  
<http://www.exploit-db.com/exploits/15746>

\* FULLDISC: 20101208 IE CSS parser dos bug  
<http://seclists.org/fulldisclosure/2010/Dec/110>

\* MISC:  
<http://www.breakingpointsystems.com/community/blog/ie-vulnerability/>

\* MISC:  
<http://www.wooyun.org/bugs/wooyun-2010-0885>

\* MISC:  
<http://www.microsoft.com/technet/security/advisory/2488013.msp>

\* MISC:  
<http://blogs.technet.com/b/srd/archive/2011/01/07/assessing-the-risk-of-public-issues-currently-being-tracked-by-the-msrc>

\* CERT-VN: VU#634956  
<http://www.kb.cert.org/vuls/id/634956>  
\* BID: 45246  
<http://www.securityfocus.com/bid/45246>  
\* SECTRACK: 1024922  
<http://www.securitytracker.com/id?1024922>  
\* SECUNIA: 42510  
<http://secunia.com/advisories/42510>  
\* VUPEN: ADV-2010-3156  
<http://www.vupen.com/english/advisories/2010/3156>  
\* SECTRACK: 1024922  
<http://www.securitytracker.com/id/1024922>

**CVE Reference:**

CVE-2010-3971 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

● **19189 Uninitialized Memory Corruption Vulnerability (CVE-2011-0035) (MS11-003/2482017) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

**References:**

\* BID: 46157  
<http://www.securityfocus.com/bid/46157>  
\* VUPEN: VUPEN/ADV-2011-0318  
<http://www.vupen.com/english/advisories/2011/0318>  
\* SECTRACK: 1024922  
<http://www.securitytracker.com/id/1024922>  
\* MS: MS11-003  
<http://www.microsoft.com/technet/security/Bulletin/MS11-003.msp>

**CVE Reference:**

CVE-2011-0035 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

● **19190 Uninitialized Memory Corruption Vulnerability (CVE-2011-0036) (MS11-003/2482017) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

**References:**

\* BID: 46158  
<http://www.securityfocus.com/bid/46158>  
\* VUPEN: VUPEN/ADV-2011-0318  
<http://www.vupen.com/english/advisories/2011/0318>  
\* SECTRACK: 1024922  
<http://www.securitytracker.com/id/1024922>  
\* MS: MS11-003  
<http://www.microsoft.com/technet/security/Bulletin/MS11-003.msp>

**CVE Reference:**

CVE-2011-0035 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 19191 Internet Explorer Insecure Library Loading Vulnerability (MS11-003/2482017) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer handles the loading of DLL files. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

#### References:

- \* BID: 46159  
<http://www.securityfocus.com/bid/46159>
- \* VUPEN: VUPEN/ADV-2011-0318  
<http://www.vupen.com/english/advisories/2011/0318>
- \* SECTRACK: 1024922  
<http://www.securitytracker.com/id/1024922>
- \* MS: MS11-003  
<http://www.microsoft.com/technet/security/Bulletin/MS11-003.msp>

#### CVE Reference:

CVE-2011-0038 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 19193 Win32k Improper User Input Validation Vulnerability (MS11-012/2479628) (Remote File Checking)

An elevation of privilege vulnerability exists in the way that Windows kernel-mode drivers validate data supplied from user mode to kernel mode. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode and take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full administrative rights.

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

#### References:

- \* MS: MS11-012  
<http://www.microsoft.com/technet/security/bulletin/ms11-012.msp>
- \* VUPEN: VUPEN/ADV-2011-0325  
<http://www.vupen.com/english/advisories/2011/0325>
- \* SECTRACK: 1025047  
<http://www.securitytracker.com/id/1025047>
- \* BID: 46141  
<http://www.securityfocus.com/bid/46141>

#### CVE Reference:

CVE-2011-0086 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 19194 Win32k Insufficient User Input Validation Vulnerability (MS11-012/2479628) (Remote File Checking)

An elevation of privilege vulnerability exists in the way that Windows kernel-mode drivers validate data supplied from user mode to kernel mode. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode and take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full administrative rights.

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

#### References:

- \* MS: MS11-012  
<http://www.microsoft.com/technet/security/bulletin/ms11-012.msp>
- \* VUPEN: VUPEN/ADV-2011-0325  
<http://www.vupen.com/english/advisories/2011/0325>
- \* SECTRACK: 1025047  
<http://www.securitytracker.com/id/1025047>
- \* BID: 46148  
<http://www.securityfocus.com/bid/46148>

#### CVE Reference:

CVE-2011-0087 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 19195 Win32k Window Class Pointer Confusion Vulnerability (MS11-012/2479628) (Remote File Checking)

An elevation of privilege vulnerability exists in the way that Windows kernel-mode drivers validate data supplied from user mode to kernel mode. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode and take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full administrative rights.

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

#### References:

- \* MS: MS11-012  
<http://www.microsoft.com/technet/security/bulletin/ms11-012.msp>
- \* VUPEN: VUPEN/ADV-2011-0325  
<http://www.vupen.com/english/advisories/2011/0325>
- \* SECTRACK: 1025047  
<http://www.securitytracker.com/id/1025047>
- \* BID: 46147  
<http://www.securityfocus.com/bid/46147>

#### CVE Reference:

CVE-2011-0088 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 19196 Win32k Window Class Improper Pointer Validation Vulnerability (MS11-012/2479628) (Remote File Checking)

An elevation of privilege vulnerability exists in the way that Windows kernel-mode drivers validate data supplied from user mode to kernel mode. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode and take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full administrative rights.

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

#### References:

- \* MS: MS11-012  
<http://www.microsoft.com/technet/security/bulletin/ms11-012.msp>
- \* VUPEN: VUPEN/ADV-2011-0325  
<http://www.vupen.com/english/advisories/2011/0325>
- \* SECTRACK: 1025047  
<http://www.securitytracker.com/id/1025047>
- \* BID: 46149  
<http://www.securityfocus.com/bid/46149>

#### CVE Reference:

CVE-2011-0089 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 19197 Win32k Memory Corruption Vulnerability (MS11-012/2479628) (Remote File Checking)

An elevation of privilege vulnerability exists in the way that Windows kernel-mode drivers validate data supplied from user mode to kernel mode. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode and take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full administrative rights.

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

#### References:

- \* MS: MS11-012  
<http://www.microsoft.com/technet/security/bulletin/ms11-012.msp>
- \* VUPEN: VUPEN/ADV-2011-0325  
<http://www.vupen.com/english/advisories/2011/0325>
- \* SECTRACK: 1025047  
<http://www.securitytracker.com/id/1025047>
- \* BID: 46150  
<http://www.securityfocus.com/bid/46150>

#### CVE Reference:

CVE-2011-0090 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

# New Vulnerabilities found this Week

## • CVE-2011-0033 Microsoft CVSS 2.0 Score = 9.3

The OpenType Compact Font Format (CFF) driver in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate parameter values in OpenType fonts, which allows remote attackers to execute arbitrary code via a crafted font, aka "OpenType Font Encoded Character Vulnerability."

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

### References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-007.msp>

CVE Reference: [CVE-2011-0033](#)

## • CVE-2011-0035 Microsoft CVSS 2.0 Score = 9.3

Microsoft Internet Explorer 6, 7, and 8 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, leading to memory corruption, aka "Uninitialized Memory Corruption Vulnerability," a different vulnerability than CVE-2010-2556 and CVE-2011-0036.

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

### References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-003.msp>

CVE Reference: [CVE-2011-0035](#)

## • CVE-2011-0036 Microsoft CVSS 2.0 Score = 9.3

Microsoft Internet Explorer 6, 7, and 8 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, leading to memory corruption, aka "Uninitialized Memory Corruption Vulnerability," a different vulnerability than CVE-2010-2556 and CVE-2011-0035.

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

### References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-003.msp>

CVE Reference: [CVE-2011-0036](#)

## • CVE-2011-0038 Microsoft CVSS 2.0 Score = 9.3

Untrusted search path vulnerability in Microsoft Internet Explorer 8 might allow local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a Desktop directory that contains an HTML file, aka "Internet Explorer Insecure Library Loading Vulnerability."

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

### References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-003.msp>

CVE Reference: [CVE-2011-0038](#)

## • CVE-2011-0039 Microsoft CVSS 2.0 Score = 7.2

The Local Security Authority Subsystem Service (LSASS) in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly process authentication requests, which allows local users to gain privileges via a request with a crafted length, aka "LSASS Length Validation Vulnerability."

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

### References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-014.msp>

CVE Reference: [CVE-2011-0039](#)

## • CVE-2011-0045 Microsoft CVSS 2.0 Score = 7.2

The kernel in Microsoft Windows XP SP3 performs memory allocation before properly validating unspecified data obtained from a user, which allows local users to gain privileges via a crafted application, aka "Windows Kernel Integer Truncation Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-011.msp>

**CVE Reference:** [CVE-2011-0045](#)

• **CVE-2011-0086 Microsoft CVSS 2.0 Score = 7.2**

win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka "Win32k Improper User Input Validation Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-012.msp>

**CVE Reference:** [CVE-2011-0086](#)

• **CVE-2011-0087 Microsoft CVSS 2.0 Score = 7.2**

win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 Gold and SP2 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka "Win32k Insufficient User Input Validation Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-012.msp>

**CVE Reference:** [CVE-2011-0087](#)

## **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](mailto: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](mailto: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](mailto:info-scanner@securescout.net)