

## 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

POS's often easy to hack. Cebit speaker about the importance of security education. Is satellite internet the solution against rogue countries cutting off communications? Infected apps removed from market.

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

### • Cybercriminals targeting point-of-sale devices

IDG News Service - Point-of-sale payment processing devices for credit and debit cards are proving to be rich targets for cybercriminals due to lax security controls, particularly among small businesses, according to a report from Trustwave.

Trustwave, which investigates payment card breaches for companies such as American Express, Visa and MasterCard, conducted 220 investigations worldwide involving data breaches in 2010. The vast majority of those cases came down to weaknesses in POS devices.

"Representing many targets and due to well-known vulnerabilities, POS systems continue to be the easiest method for criminals to obtain the data necessary to commit payment card fraud," according to Trustwave's Global Security Report 2011. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9212882/Cybercriminals\\_targeting\\_point\\_of\\_sale\\_devices?source=rss\\_secu](http://www.computerworld.com/s/article/9212882/Cybercriminals_targeting_point_of_sale_devices?source=rss_secu)

### • **Security: Never mind the products, educate the users**

IDG News Service - If they could change one thing to improve IT security, the assembled experts on a panel at Cebit would better educate their users.

"Education is important: We're all too naive," said Eddy Willems, global security officer for G Data Software, speaking in a panel session on security during the Cebit Global Conference, part of the Cebit trade show in Hanover, Germany, on Wednesday.

"People need to take security seriously. We can do a lot at a technological level, but if they choose a weak password, they are at risk," said Joachim Schaper, vice president of research at AGT Germany, which provides physical, as well as IT, security services. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9212578/Security\\_Never\\_mind\\_the\\_products\\_educate\\_the\\_users?source=rss](http://www.computerworld.com/s/article/9212578/Security_Never_mind_the_products_educate_the_users?source=rss)

### • **We need to ignite a Layer-1 revolution**

Network World - Egypt's revolution was heralded as a success story for social media services such as Twitter and Facebook. Western journalists fawned over every rare example of social media, ignoring the more mundane but far more at communication services such as cellular phone calls and text messaging. The really interesting story out of Egypt, and more recently Libya, Iran and other places was the communications blackouts imposed by each regime. While the west focused on layer-7 technologies, the tyrants were smart enough to strike at the root of their citizens efforts: layer-1 physical layer connectivity for phones.

Instead of glamorizing Facebook, perhaps the west needs to consider the serious implications of the ease with which these regimes are able to disconnect their countries from the world. Turns out the Internet "was designed to survive a nuclear strike", but falls easily to BGP null-routing or good old-fashioned garden shears on a few carefully selected cables. The countries that need communication redundancy and survivability the most have so few connections to the Internet that they can easily be turned off. There's a solution to this problem: satellite Internet uplinks providing local guerrilla-GSM with pico cells. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9212559/We\\_need\\_to\\_ignite\\_a\\_Layer\\_1\\_revolution?source=rss\\_security&u](http://www.computerworld.com/s/article/9212559/We_need_to_ignite_a_Layer_1_revolution?source=rss_security&u)

### • **Google yanks over 50 infected apps from Android Market**

Computerworld - Google has pulled more than 50 malware-infected apps from its Android Market, but hasn't yet triggered automatic uninstalls of those programs from users' phones, security experts said today.

"The apps were 'Trojanized,' for a better word," said Tom Parsons, a senior manager with Symantec's security response team. "With the phones being 'rooted,' the attacks can do almost anything, including pulling data off the phone," he said, referring to the malware's ability to gain root access to the devices.

The apps were available for about four days on the Android Market, Google's official app store. According to San Francisco-based smartphone security firm Lookout, between 50,000 and 200,000 copies of the apps were downloaded by users. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9212598/Google\\_yanks\\_over\\_50\\_infected\\_apps\\_from\\_Android\\_Market?source=rss](http://www.computerworld.com/s/article/9212598/Google_yanks_over_50_infected_apps_from_Android_Market?source=rss)

## **New Vulnerabilities Tested in SecureScout**

### • **14629 Adobe Acrobat / Reader library-loading vulnerability (CVE-2011-0588) (Remote File Checking)**

Untrusted search path vulnerability in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows allows local users to gain privileges via a Trojan horse DLL in the current working directory, a different vulnerability than CVE-2011-0562 and CVE-2011-0570.

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

#### **References:**

\* BID: 46254

<http://www.securityfocus.com/bid/46254>

\* SECTRACK: 1025033

<http://securitytracker.com/id/1025033>

\* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb11-03.html>

\* VUPEN: ADV-2011-0337

<http://www.vupen.com/english/advisories/2011/0337>

#### CVE Reference:

CVE-2011-0588 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 14630 Adobe Acrobat / Reader memory corruption vulnerability (CVE-2011-0589) (Remote File Checking)

Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0563 and CVE-2011-0606.

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

#### References:

\* BID: 46202

<http://www.securityfocus.com/bid/46202>

\* SECTRACK: 1025033

<http://securitytracker.com/id/1025033>

\* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb11-03.html>

\* VUPEN: ADV-2011-0337

<http://www.vupen.com/english/advisories/2011/0337>

#### CVE Reference:

CVE-2011-0589 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 14631 Adobe Acrobat / Reader 3D file parsing input validation vulnerability (CVE-2011-0590) (Remote File Checking)

Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a 3D file, a different vulnerability than CVE-2011-0591, CVE-2011-0592, CVE-2011-0593, CVE-2011-0595, and CVE-2011-0600.

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

#### References:

\* BID: 46208

<http://www.securityfocus.com/bid/46208>

\* SECTRACK: 1025033

<http://securitytracker.com/id/1025033>

\* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb11-03.html>

\* VUPEN: ADV-2011-0337

<http://www.vupen.com/english/advisories/2011/0337>

#### CVE Reference:

CVE-2011-0590 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 14632 Adobe Acrobat / Reader 3D file parsing input validation vulnerability (CVE-2011-0591) (Remote File Checking)

Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a 3D file, a different vulnerability than CVE-2011-0590, CVE-2011-0592, CVE-2011-0593, CVE-2011-0595, and CVE-2011-0600.

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

#### References:

\* BID: 46209

<http://www.securityfocus.com/bid/46209>

\* SECTRACK: 1025033

<http://securitytracker.com/id/1025033>

\* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb11-03.html>

\* VUPEN: ADV-2011-0337

<http://www.vupen.com/english/advisories/2011/0337>

#### CVE Reference:

CVE-2011-0591 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **14633 Adobe Acrobat / Reader 3D file parsing input validation vulnerability (CVE-2011-0592) (Remote File Checking)**

Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a 3D file, a different vulnerability than CVE-2011-0590, CVE-2011-0591, CVE-2011-0593, CVE-2011-0595, and CVE-2011-0600.

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

**References:**

- \* BID: 46210  
<http://www.securityfocus.com/bid/46210>
- \* SECTRACK: 1025033  
<http://securitytracker.com/id/1025033>
- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb11-03.html>
- \* VUPEN: ADV-2011-0337  
<http://www.vupen.com/english/advisories/2011/0337>

**CVE Reference:**

CVE-2011-0592 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **14634 Adobe Acrobat / Reader 3D file parsing input validation vulnerability (CVE-2011-0593) (Remote File Checking)**

Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a 3D file, a different vulnerability than CVE-2011-0590, CVE-2011-0591, CVE-2011-0592, CVE-2011-0595, and CVE-2011-0600.

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

**References:**

- \* BID: 46211  
<http://www.securityfocus.com/bid/46211>
- \* SECTRACK: 1025033  
<http://securitytracker.com/id/1025033>
- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb11-03.html>
- \* VUPEN: ADV-2011-0337  
<http://www.vupen.com/english/advisories/2011/0337>

**CVE Reference:**

CVE-2011-0593 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **14635 Adobe Acrobat / Reader font parsing input validation vulnerability (CVE-2011-0594) (Remote File Checking)**

Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a font.

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

**References:**

- \* BID: 46216  
<http://www.securityfocus.com/bid/46216>
- \* SECTRACK: 1025033  
<http://securitytracker.com/id/1025033>
- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb11-03.html>
- \* VUPEN: ADV-2011-0337  
<http://www.vupen.com/english/advisories/2011/0337>

**CVE Reference:**

CVE-2011-0594 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **14636 Adobe Acrobat / Reader 3D file parsing input validation vulnerability (CVE-2011-0595) (Remote File Checking)**

Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a 3D file, a different vulnerability than CVE-2011-0590, CVE-2011-0591, CVE-2011-0592, CVE-2011-0593, and CVE-2011-0600.

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

#### References:

- \* BID: 46212  
<http://www.securityfocus.com/bid/46212>
- \* SECTRACK: 1025033  
<http://securitytracker.com/id/1025033>
- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb11-03.html>
- \* VUPEN: ADV-2011-0337  
<http://www.vupen.com/english/advisories/2011/0337>

#### CVE Reference:

CVE-2011-0595 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 14637 Adobe Acrobat / Reader image parsing input validation vulnerability (CVE-2011-0596) (Remote File Checking)

Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via an image, a different vulnerability than CVE-2011-0598, CVE-2011-0599, and CVE-2011-0602.

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

#### References:

- \* BID: 46218  
<http://www.securityfocus.com/bid/46218>
- \* SECTRACK: 1025033  
<http://securitytracker.com/id/1025033>
- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb11-03.html>
- \* VUPEN: ADV-2011-0337  
<http://www.vupen.com/english/advisories/2011/0337>

#### CVE Reference:

CVE-2011-0596 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19176 Cisco IOS Software cable-docsis community string vulnerability (CSCdr59314)

Implementation of new cable-industry standards for management of cable modems introduced an undocumented read-write community string, "cable-docsis", which was intended only for DOCSIS-compliant cable-capable devices. It was inadvertently enabled by default for all devices except DOCSIS-compatible cable modems and head end units in a limited range of IOS releases. This defect is documented as CSCdr59314. This vulnerability is confined to a very narrow set of IOS releases based on 12.1(3) and 12.1(3)T, and it is fixed in 12.1(4) and 12.1(5)T releases and following.

This vulnerability could be exploited to gain access to or modify the configuration and operation of any affected devices without authorization.

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

#### References:

- \* CISCO: 20041008 Cisco IOS Software Multiple SNMP Community String Vulnerabilities  
<http://www.cisco.com/warp/public/707/ios-snmp-community-vulns-pub.shtml>
- \* CERT-VN: VU#840665  
<http://www.kb.cert.org/vuls/id/840665>
- \* XF: cisco-ios-cable-docsis(6180)  
<http://xforce.iss.net/xforce/xfdb/6180>

#### CVE Reference:

CVE-2004-1776 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

• **CVE-2011-0278 HP CVSS 2.0 Score = 4.3**

Unspecified vulnerability in HP Web Jetadmin 10.2 Service Release 3 and 4 allows local users to bypass intended access restrictions via unknown vectors.

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

**References:**

VUPEN: <http://www.vupen.com/english/advisories/2011/0516>

SECTRAK: <http://securitytracker.com/id?1025130>

SECUNIA: <http://secunia.com/advisories/43526>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02714670>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02714670>

**CVE Reference:** [CVE-2011-0278](#)

• **CVE-2011-1106 IBM CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in stcenter.nsf in the server in IBM Lotus Sametime allows remote attackers to inject arbitrary web script or HTML via the authReasonCode parameter in an OpenDatabase action.

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

**References:**

XF: <http://xforce.iss.net/xforce/xfdb/65555>

BID: <http://www.securityfocus.com/bid/46481>

SECUNIA: <http://secunia.com/advisories/43430>

BUGTRAQ: <http://archives.neohapsis.com/archives/bugtraq/2011-02/0217.html>

**CVE Reference:** [CVE-2011-1106](#)

• **CVE-2011-0925 Cisco CVSS 2.0 Score = 9.3**

The CSDWebInstallerCtrl ActiveX control in CSDWebInstaller.ocx in Cisco Secure Desktop (CSD) allows remote attackers to download an unintended Cisco program onto a client machine, and execute this program, by identifying a Cisco program with a Cisco digital signature and then renaming this program to inst.exe, a different vulnerability than CVE-2010-0589 and CVE-2011-0926.

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

**References:**

MISC: <http://zerodayinitiative.com/advisories/ZDI-11-092/>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/516648/100/0/threaded>

**CVE Reference:** [CVE-2011-0925](#)

• **CVE-2011-1017 Linux CVSS 2.0 Score = 7.2**

Heap-based buffer overflow in the ldm\_frag\_add function in fs/partitions/ldm.c in the Linux kernel 2.6.37.2 and earlier might allow local users to gain privileges or obtain sensitive information via a crafted LDM partition table.

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

**References:**

MISC: <http://www.pre-cert.de/advisories/PRE-SA-2011-01.txt>

SECTRAK: <http://securitytracker.com/id?1025128>

MLIST: <http://openwall.com/lists/oss-security/2011/02/24/4>

MLIST: <http://openwall.com/lists/oss-security/2011/02/24/14>

MLIST: <http://openwall.com/lists/oss-security/2011/02/23/16>

**CVE Reference:** [CVE-2011-1017](#)

• **CVE-2011-1016 Linux CVSS 2.0 Score = 6.9**

The Radeon GPU drivers in the Linux kernel before 2.6.38-rc5 do not properly validate data related to the AA resolve registers, which allows local users to write to arbitrary memory locations associated with (1) Video RAM (aka VRAM) or (2) the Graphics Translation Table (GTT) via crafted values.

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

**References:**

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=680000](https://bugzilla.redhat.com/show_bug.cgi?id=680000)

MLIST: <http://openwall.com/lists/oss-security/2011/02/25/4>

MLIST: <http://openwall.com/lists/oss-security/2011/02/24/3>

MLIST: <http://openwall.com/lists/oss-security/2011/02/24/11>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=fff1ce4dc6113b6fdc4e3a815ca5fd229408f8ef>

BID: <http://www.securityfocus.com/bid/46557>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.38-rc5>

**CVE Reference:** [CVE-2011-1016](#)

• **CVE-2011-1010 Linux CVSS 2.0 Score = 4.9**

Buffer overflow in the mac\_partition function in fs/partitions/mac.c in the Linux kernel before 2.6.37.2 allows local users to cause a denial of service (panic) or possibly have unspecified other impact via a malformed Mac OS partition table.

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

**References:**

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=679282](https://bugzilla.redhat.com/show_bug.cgi?id=679282)

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=fa7ea87a057958a8b7926c1a60a3ca6d696328ed>

MISC: <http://www.pre-cert.de/advisories/PRE-SA-2011-01.txt>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.37.2>

MLIST: <http://openwall.com/lists/oss-security/2011/02/22/3>

MLIST: <http://openwall.com/lists/oss-security/2011/02/22/15>

MLIST: <http://openwall.com/lists/oss-security/2011/02/22/11>

**CVE Reference:** [CVE-2011-1010](#)

• **CVE-2011-1012 Linux CVSS 2.0 Score = 4.9**

The ldm\_parse\_vmdb function in fs/partitions/ldm.c in the Linux kernel before 2.6.38-rc6-git6 does not validate the VBLK size value in the VMDB structure in an LDM partition table, which allows local users to cause a denial of service (divide-by-zero error and OOPS) via a crafted partition table.

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

**References:**

MLIST: <http://www.spinics.net/lists/mm-commits/msg82429.html>

MLIST: <http://openwall.com/lists/oss-security/2011/02/23/4>

MLIST: <http://openwall.com/lists/oss-security/2011/02/23/21>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=294f6cf48666825d23c9372ef37631232746e40d>

MISC: <http://www.pre-cert.de/advisories/PRE-SA-2011-01.txt>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/snapshots/patch-2.6.38-rc6-git6.log>

**CVE Reference:** [CVE-2011-1012](#)

• **CVE-2011-1020 Linux CVSS 2.0 Score = 2.1**

The proc filesystem implementation in the Linux kernel 2.6.37 and earlier does not restrict access to the /proc directory tree of a process after this process performs an exec of a setuid program, which allows local users to obtain sensitive information or cause a denial of service via open, lseek, read, and write system calls.

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

**References:**

MLIST: <https://lkml.org/lkml/2011/2/9/417>

MLIST: <https://lkml.org/lkml/2011/2/7/474>

MLIST: <https://lkml.org/lkml/2011/2/7/466>

MLIST: <https://lkml.org/lkml/2011/2/7/414>

MLIST: <https://lkml.org/lkml/2011/2/7/404>

MLIST: <https://lkml.org/lkml/2011/2/7/368>

MLIST: <https://lkml.org/lkml/2011/2/10/21>

MISC: <http://www.halfdog.net/Security/2011/SuidBinariesAndProcInterface/>

SECUNIA: <http://secunia.com/advisories/43496>

FULLDISC: <http://seclists.org/fulldisclosure/2011/Jan/421>

MLIST: <http://openwall.com/lists/oss-security/2011/02/25/2>

MLIST: <http://openwall.com/lists/oss-security/2011/02/24/18>

**CVE Reference:** [CVE-2011-1020](#)

**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)