

## 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

Security budgets lagging. IRS security not good enough. 4.2 million Sutter Health patients' personal information stolen. Rumanian accused of hacking NASA.

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

### • SC Congress New York: Attacks increasing, budgets lagging

As the threat landscape worsens, efforts by security professionals to defend networks are hampered by tight budgets, participants on a panel, "Running on empty," agreed at Wednesday's SC Congress New York. "Welcome to my life over the past eight years," said Andrew Stravitz, who until recently was director of information security for barnesandnoble.com. He detailed some of the steps he made for the online operations of the book retailer, which boiled down to doing more with less. Initially, assisted by only two interns, he was able to build up a network operations center, develop strong policies and procedures, grow the number of customer service representatives from 500 to 1,000 worldwide, and strengthen the company's corporate social responsibility (CSR) program.

Needing to comply with PCI regulations allowed&nbsp;Stravitz to get the budget required to build out this infrastructure, he said. He convinced his bosses of the need for a server and engineering group to protect customers' personally identifiable information and credit card numbers, for example, which he achieved by hiding data in a secure VLAN. The point was to develop security with the assumption that the network would be breached, so his focus was on protecting the data with cryptographic defenses. SC Magazine

Full Story :

[http://www.scmagazineus.com/sc-congress-new-york-attacks-increasing-budgets-lagging/article/217012/?utm\\_source=](http://www.scmagazineus.com/sc-congress-new-york-attacks-increasing-budgets-lagging/article/217012/?utm_source=)

### • GAO again slams IRS over security weaknesses

After repeatedly sounding the alarm about lax data security practices at the Internal Revenue Service (IRS), the U.S. Government Accountability Office (GAO) again has warned that the nation's tax collector is operating with significant deficiencies.

While the IRS has made strides to address previously reported issues, the majority of known security weaknesses have not yet been fixed, according to a financial audit report to the secretary of the treasury, released Tuesday. As was the case in the past, many of the network weaknesses turned up in the latest audit were related to system access and configuration controls.

The IRS, for example, relies on a procurement system that lacks the appropriate access controls and database maintenance. In addition, the IRS still uses unencrypted protocols for a sensitive, tax-processing application. SC Magazine

Full Story :

[http://www.scmagazineus.com/gao-again-slams-irs-over-security-weaknesses/article/216753/?utm\\_source=feedburn](http://www.scmagazineus.com/gao-again-slams-irs-over-security-weaknesses/article/216753/?utm_source=feedburn)

### • Sutter Health loses computer, data on 4.2 million

A desktop computer stolen from a Northern California health care system contained the personal information of roughly 4.2 million patients, the organization revealed Wednesday.

Sutter Health, a nonprofit network of doctors and hospitals serving 100 communities, said in a notice to patients that the computer was not encrypted when it was stolen Oct. 17 from Sutter's headquarters in Sacramento.

A database on the computer housed the names, addresses, birth dates, phone numbers, and medical record numbers of 3.3 million patients of Sutter Physician Services, which provides billing and managed care services for various health care providers. Also included were the names of the patient's health insurance plan. The assets were recorded beginning in 1995 until January of this year. SC Magazine

Full Story :

[http://www.scmagazineus.com/sutter-health-loses-computer-data-on-42-million/article/216983/?utm\\_source=feedburn](http://www.scmagazineus.com/sutter-health-loses-computer-data-on-42-million/article/216983/?utm_source=feedburn)

### • Romanian hacker accused of breaking into NASA server

Police in Romania this week arrested a 26-year-old hacker accused of breaking into several servers belonging to NASA, and causing hundreds of thousands of dollars in damages. Robert Butyka was detained Tuesday in Cluj Napoca, Romania's fourth most populated city, according to a news release issued by Romania's Directorate for Investigating Organized Crime and Terrorism (DIICOT). Butyka, who reportedly used the online alias "Iceman," allegedly hacked into NASA's servers beginning in Dec. 2010.

He then purportedly damaged data on the systems and restricted access to the information, causing major disruptions, according to Romanian authorities. Damage from Butyka's alleged actions cost the U.S. space agency \$500,000.

Butyka faces various computer crime charges, including obtaining unauthorized access and causing serious disruption to a computer system, restricting access to data without authorization, and possessing hacking programs. SC Magazine

Full Story :

[http://www.scmagazineus.com/romanian-hacker-accused-of-breaking-into-nasa-server/article/217019/?utm\\_source=](http://www.scmagazineus.com/romanian-hacker-accused-of-breaking-into-nasa-server/article/217019/?utm_source=)

## New Vulnerabilities Tested in SecureScout

### • 13827 Oracle Database Server - Database Vault 'DV\_ACCTMGR' Privileges Remote Security Bypass Vulnerability (oct-2011/CVE-2011-3511)

Oracle Database Server is prone to a remote security-bypass vulnerability in Database Vault.

The vulnerability can be exploited over the 'Oracle Net' protocol. For an exploit to succeed, the attacker must have 'Privileged Account' privileges.

An attacker can exploit this issue to bypass certain security protections and change any user's password. Successfully exploiting this issue may lead to other attacks.

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

References:

\* CONFIRM:

<http://www.oracle.com/technetwork/topics/security/cpuoct2011-330135.html>

\* MISC:

<http://www.teamshatter.com/topics/general/team-shatter-exclusive/sql-injection-vulnerability-in-oracle-drop-index-for-spatial>

\* MISC:

<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3511>

#### CVE Reference:

CVE-2011-3511 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 13828 Oracle Database Server - 'CTXSYS.DRVDISP' Buffer Overflow Vulnerability (oct-2011/CVE-2011-2301)

Oracle Database is prone to a buffer-overflow vulnerability that exists in Oracle Text.

The vulnerability can be exploited over the 'Oracle Net' protocol. For an exploit to succeed, the attacker must have 'Execute on CTXSYS.DRVDISP' privileges.

Successful exploits will allow attackers to execute arbitrary code in the context of the affected application. This may facilitate a complete system compromise.

This vulnerability affects the following supported versions:

10.1.0.5, 10.2.0.3, 10.2.0.4, 11.1.0.7ww

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

#### References:

\* MISC:

<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-2301>

\* CONFIRM:

<http://www.oracle.com/technetwork/topics/security/cpuoct2011-330135.html>

\* BID: 50199

<http://www.securityfocus.com/bid/50199/info>

#### CVE Reference:

CVE-2011-2301 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19574 PHP 'OpenSSL' Extension Multiple Denial of Service Vulnerabilities

PHP is prone to multiple remote denial-of-service vulnerabilities that affect the 'OpenSSL' extension.

Multiple memory leaks in the OpenSSL extension in PHP before 5.3.6 might allow remote attackers to cause a denial of service (memory consumption) via (1) plaintext data to the openssl\_encrypt function or (2) ciphertext data to the openssl\_decrypt function.

Successful attacks will cause the application to consume excessive memory, creating a denial-of-service condition.

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

#### References:

\* CONFIRM:

<http://bugs.php.net/bug.php?id=54060>

\* CONFIRM:

<http://bugs.php.net/bug.php?id=54061>

\* CONFIRM:

<http://www.php.net/ChangeLog-5.php>

\* CONFIRM:

<http://support.apple.com/kb/HT5002>

\* APPLE: APPLE-SA-2011-10-12-3

<http://lists.apple.com/archives/Security-announce/2011/Oct/msg00003.html>

\* MANDRIVA: MDVSA-2011:053

<http://www.mandriva.com/security/advisories?name=MDVSA-2011:053>

\* BID: 46977

<http://www.securityfocus.com/bid/46977>

\* VUPEN: ADV-2011-0744

<http://www.vupen.com/english/advisories/2011/0744>

#### CVE Reference:

CVE-2011-1468 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## • 19575 PHP 'socket\_connect()' Function Stack Buffer Overflow Vulnerability

PHP is prone to a stack-based buffer-overflow vulnerability because the application fails to perform adequate boundary checks on user-supplied input.

Stack-based buffer overflow in the socket\_connect function in ext/sockets/sockets.c might allow context-dependent attackers to execute arbitrary code via a long pathname for a UNIX socket.

An attacker can exploit this issue to execute arbitrary machine code in the context of the PHP process. Failed exploit attempts will likely crash the webserver, denying service to legitimate users.

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

### References:

- \* EXPLOIT-DB: 17318  
<http://www.exploit-db.com/exploits/17318/>
- \* MLIST: [oss-security] 20110523 CVE request: PHP socket\_connect() - stack buffer overflow  
<http://openwall.com/lists/oss-security/2011/05/24/1>
- \* MLIST: [oss-security] 20110524 Re: CVE request: PHP socket\_connect() - stack buffer overflow  
<http://openwall.com/lists/oss-security/2011/05/24/9>
- \* CONFIRM:  
<http://svn.php.net/viewvc/php/php-src/trunk/ext/sockets/sockets.c?r1=311369&r2=311368&pathrev=311369>
- \* CONFIRM:  
<http://svn.php.net/viewvc?view=revision&revision=311369>
- \* CONFIRM:  
<http://www.php.net/ChangeLog-5.php#5.3.7>
- \* CONFIRM:  
<http://www.php.net/archive/2011.php#id2011-08-18-1>
- \* BID: 49241  
<http://www.securityfocus.com/bid/49241>
- \* OSVDB: 72644  
<http://osvdb.org/72644>
- \* SREASON: 8262  
<http://securityreason.com/securityalert/8262>
- \* SREASON: 8294  
<http://securityreason.com/securityalert/8294>
- \* XF: php-socketconnect-bo(67606)  
<http://xforce.iss.net/xforce/xfdb/67606>

### CVE Reference:

CVE-2011-1938 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## • 19576 PHP Exif Extension 'exif\_read\_data()' Function Remote Denial of Service Vulnerability

PHP is prone to a denial-of-service vulnerability that affects the Exif extension.

exif.c in the Exif extension in PHP before 5.3.6 on 64-bit platforms performs an incorrect cast, which allows remote attackers to cause a denial of service (application crash) via an image with a crafted Image File Directory (IFD) that triggers a buffer over-read.

Successfully exploiting this vulnerability allows remote attackers to cause denial-of-service conditions in the context of an application using the vulnerable extension.

NOTE: this issue affects only 64-bit platforms.

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

### References:

- \* EXPLOIT-DB: 16261  
<http://www.exploit-db.com/exploits/16261/>
- \* MLIST: [oss-security] 20110214 PHP Exif 64bit Casting Vulnerability, CVE request  
<http://openwall.com/lists/oss-security/2011/02/14/1>
- \* MLIST: [oss-security] 20110216 Re: Re: PHP Exif 64bit Casting Vulnerability, CVE request  
<http://openwall.com/lists/oss-security/2011/02/16/7>
- \* CONFIRM:  
<http://bugs.php.net/bug.php?id=54002>
- \* CONFIRM:  
<http://svn.php.net/viewvc?view=revision&revision=308316>
- \* CONFIRM:

<http://www.php.net/ChangeLog-5.php>

\* CONFIRM:

<http://www.php.net/archive/2011.php>

\* CONFIRM:

[http://www.php.net/releases/5\\_3\\_6.php](http://www.php.net/releases/5_3_6.php)

\* CONFIRM:

[https://bugzilla.redhat.com/show\\_bug.cgi?id=680972](https://bugzilla.redhat.com/show_bug.cgi?id=680972)

\* CONFIRM:

<http://support.apple.com/kb/HT5002>

\* APPLE: APPLE-SA-2011-10-12-3

<http://lists.apple.com/archives/Security-announce/2011/Oct/msg00003.html>

\* DEBIAN: DSA-2266

<http://www.debian.org/security/2011/dsa-2266>

\* FEDORA: FEDORA-2011-3614

<http://lists.fedoraproject.org/pipermail/package-announce/2011-March/056642.html>

\* FEDORA: FEDORA-2011-3636

<http://lists.fedoraproject.org/pipermail/package-announce/2011-April/057709.html>

\* FEDORA: FEDORA-2011-3666

<http://lists.fedoraproject.org/pipermail/package-announce/2011-April/057710.html>

\* MANDRIVA: MDVSA-2011:052

<http://www.mandriva.com/security/advisories?name=MDVSA-2011:052>

\* MANDRIVA: MDVSA-2011:053

<http://www.mandriva.com/security/advisories?name=MDVSA-2011:053>

\* BID: 46365

<http://www.securityfocus.com/bid/46365>

\* SREASON: 8114

<http://securityreason.com/securityalert/8114>

\* VUPEN: ADV-2011-0744

<http://www.vupen.com/english/advisories/2011/0744>

\* VUPEN: ADV-2011-0764

<http://www.vupen.com/english/advisories/2011/0764>

\* VUPEN: ADV-2011-0890

<http://www.vupen.com/english/advisories/2011/0890>

#### CVE Reference:

CVE-2011-0708 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19580 Adobe Flash Player Stack-based buffer overflow in the ActionScript Virtual Machine CVE-2011-2426

Stack-based buffer overflow in the ActionScript Virtual Machine (AVM) component in Adobe Flash Player before 10.3.183.10 on Windows, allows remote attackers to execute arbitrary code via unspecified vectors.

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

#### References:

\* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb11-26.html>

\* REDHAT: RHSA-2011:1333

<http://www.redhat.com/support/errata/RHSA-2011-1333.html>

\* SUSE: SUSE-SU-2011:1063

<http://lists.opensuse.org/opensuse-security-announce/2011-09/msg00025.html>

#### CVE Reference:

CVE-2011-2426 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19581 Adobe Flash Player Stack-based buffer overflow in the ActionScript Virtual Machine CVE-2011-2427

Stack-based buffer overflow in the ActionScript Virtual Machine (AVM) component in Adobe Flash Player before 10.3.183.10 on Windows allows attackers to execute arbitrary code or cause a denial of service via unspecified vectors.

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

#### References:

\* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb11-26.html>

\* REDHAT: RHSA-2011:1333

<http://www.redhat.com/support/errata/RHSA-2011-1333.html>

\* SUSE: SUSE-SU-2011:1063

<http://lists.opensuse.org/opensuse-security-announce/2011-09/msg00025.html>

#### CVE Reference:

CVE-2011-2427 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19582 Adobe Flash Player denial of service via unspecified vectors related to a "logic error issue."

Adobe Flash Player before 10.3.183.10 on Windows allows attackers to execute arbitrary code or cause a denial of service (browser crash) via unspecified vectors, related to a "logic error issue."

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

#### References:

\* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb11-26.html>

\* REDHAT: RHSA-2011:1333

<http://www.redhat.com/support/errata/RHSA-2011-1333.html>

\* SUSE: SUSE-SU-2011:1063

<http://lists.opensuse.org/opensuse-security-announce/2011-09/msg00025.html>

#### CVE Reference:

CVE-2011-2428 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19583 Adobe Flash Player denial of service via unspecified vectors related to a "security control bypass."

Adobe Flash Player before 10.3.183.10 on Windows allows attackers to execute arbitrary code or cause a denial of service (browser crash) via unspecified vectors, related to a "logic error issue."

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

#### References:

NULL

#### CVE Reference:

CVE-2011-2429 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19584 Adobe Flash Player arbitrary code related to a "logic error vulnerability."

Adobe Flash Player before 10.3.183.10 on Windows allows remote attackers to execute arbitrary code via crafted streaming media, related to a "logic error vulnerability."

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

#### References:

\* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb11-26.html>

\* REDHAT: RHSA-2011:1333

<http://www.redhat.com/support/errata/RHSA-2011-1333.html>

\* SUSE: SUSE-SU-2011:1063

<http://lists.opensuse.org/opensuse-security-announce/2011-09/msg00025.html>

#### CVE Reference:

CVE-2011-2430 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19585 Adobe Flash Player Cross-site scripting (XSS) vulnerability via a crafted URL related to a "universal cross-site scripting issue,"

Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 10.3.183.10 on Windows allows remote attackers to inject arbitrary web script or HTML via a crafted URL, related to a "universal cross-site scripting issue," as exploited in the wild in September 2011.

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

#### References:

\* CONFIRM:

[http://googlechromereleases.blogspot.com/2011/09/stable-channel-update\\_20.html](http://googlechromereleases.blogspot.com/2011/09/stable-channel-update_20.html)

\* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb11-26.html>

\* REDHAT: RHSA-2011:1333

<http://www.redhat.com/support/errata/RHSA-2011-1333.html>

\* SUSE: SUSE-SU-2011:1063

<http://lists.opensuse.org/opensuse-security-announce/2011-09/msg00025.html>

**CVE Reference:**

CVE-2011-2444 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

• **CVE-2011-4157 HP CVSS 2.0 Score = 10.0**

Stack-based buffer overflow in hydra.exe in HP SAN/iQ before 9.5 on the HP StorageWorks P4000 Virtual SAN Appliance allows remote attackers to execute arbitrary code via a crafted login request.

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

**References:**

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-11-111/>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03082086>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03082086>

**CVE Reference:** [CVE-2011-4157](#)

• **CVE-2011-4156 HP CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in HP Network Node Manager i (NNMi) 9.0x and 9.1x allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2011-4155.

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

**References:**

HP: <http://www.securityfocus.com/archive/1/520459>

HP: <http://www.securityfocus.com/archive/1/520459>

**CVE Reference:** [CVE-2011-4156](#)

• **CVE-2011-4155 HP CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in HP Network Node Manager i (NNMi) 9.0x and 9.1x allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2011-4156.

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

**References:**

HP: <http://www.securityfocus.com/archive/1/520459>

HP: <http://www.securityfocus.com/archive/1/520459>

**CVE Reference:** [CVE-2011-4155](#)

• **CVE-2011-4158 HP CVSS 2.0 Score = 4.0**

Unspecified vulnerability in HP Directories Support for ProLiant Management Processors 3.10 and 3.20 for Integrated Lights-Out iLO2 and iLO3 allows remote authenticated users to obtain sensitive information via unknown vectors.

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

**References:**

HP: <http://www.securityfocus.com/archive/1/archive/1/520484/100/0/threaded>

HP: <http://www.securityfocus.com/archive/1/archive/1/520484/100/0/threaded>

**CVE Reference:** [CVE-2011-4158](#)

• **CVE-2011-1516 Apple CVSS 2.0 Score = 7.5**

The kSBXProfileNoNetwork and kSBXProfileNoInternet sandbox profiles in Apple Mac OS X 10.5.x through 10.7.x do not propagate restrictions to all created processes, which allows remote attackers to access network resources via a crafted application, as demonstrated by use of osascript to send Apple events to the launchd daemon, a related issue to CVE-2008-7303.

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

**References:**

MISC: <http://www.coresecurity.com/content/apple-osx-sandbox-bypass>

**CVE Reference:** [CVE-2011-1516](#)

• **CVE-2008-7303 Apple CVSS 2.0 Score = 7.5**

The nonet and nointernet sandbox profiles in Apple Mac OS X 10.5.x do not propagate restrictions to all created processes, which allows remote attackers to access network resources via a crafted application, as demonstrated by use of launchctl to trigger the launchd daemon's execution of a script file, a related issue to CVE-2011-1516.

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

**References:**

MISC: <https://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Miller/BlackHat-Japan-08-Miller-Hacking-OSX.pdf>

MISC: <http://www.coresecurity.com/content/apple-osx-sandbox-bypass>

**CVE Reference:** [CVE-2008-7303](#)

**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)