

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

[Messenger Service Vulnerability Scanner](#) – The Messenger Service 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 Microsoft Windows Messenger Service flaw (MS03-043).

This Week in Review

This week netVigilance Security Research has found 3 vulnerabilities in open source software Jetbox Contents Management System:

1 high risk, 1 medium risk and 1 low risk. The vulnerabilities include SQL Injection, XSS (Cross site Scripting) and Path Disclosure Vulnerabilities.

To see details and further information please see:

<http://www.netvigilance.com/advisories>

netvigilance releases WinHoneyd 1.5 with all the features of Honeyd. We also offer a commercial GUI for those not interested in dealing with complex configurations.

This is how infoworld reacts:

Honeyd Fixed and Ported to Windows

I could not be more excited. Years ago, Michael Davis ported an early version of Honeyd (www.honeyd.org) to Windows as part of a Honeyd contest. It was an admirable attempt, but contained so many bugs that it really couldn't be used as a proper honeypot. As Windows changed versions, the older, ported, version of Honeyd remained the same, with bugs and less features than it's Linux/Unix/BSD counterpart. Every since my book, Honeypots for Windows, was published, I've been recommending Honeyd on Linux or OpenBSD for users who want to use Honeyd. Since most Windows users don't have nix

skills, it was a lot to ask.

It was announced today that Jesper Jurcenoks with netVigilance has ported the latest, and feature rich version of Honeyd, and it is available for free download (registration is required).

They have also created an optional \$99 GUI configurator. If you're new to Honeyd and want to have less problems, buy the gui and support the vendor.

infoworld

http://weblog.infoworld.com/securityadviser/archives/2007/05/honeyd_fixed_an.html

PCI Security Standard Council advisors named. How to secure your browser. Google and privacy. Domainkey new security technology.

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

❖ Credit card giant name their online security advisers

The PCI Security Standards Council, the private regulatory group run by the major credit card companies, has named its first board of advisers.

The 14-member board includes Wal-Mart, Tesco, and several banks including Bank of America and JP Morgan Chase. Bob Russo, general manager of the PCI SSC, said the elected board also will include seven members from the executive committee of the founders of the organisation, Visa, MasterCard and American Express.

"This is our first advisory board, and the types of things we will be looking for are having them advise us on security issues in their markets and relaying modifications and refinements to the PCI standard," Russo said.

The payment-card companies that founded PCI SSC have sought to require any business processing credit and debit cards to support the PCI security standard, but they have not been entirely successful.

computerworlduk

Full Story :

<http://www.computerworlduk.com/technology/security-products/authentication/news/index.cfm?RSS&newsid=3180>

❖ Internet Explorer security learning guide

Web browsers can serve as a gateway for malicious hackers who want to infect your network if not it is not properly secured. As the most commonly used Web browser,

Internet Explorer is a popular target for these hackers.

In this Web browser security guide, check out the layers of Internet Explorer security, tips on security Internet Explorer versions 6.0 and 7.0 and how to properly configure your Web browsers for optimum security. Internet Explorer 7

Touted as the most secure version of the Web browser to date, it goes without saying that Internet Explorer 7 (IE7) is not hacker proof. Internet Explorer 7's features are designed to prevent viruses, spyware and other forms of malware from infecting your Windows system. With cross-site scripting protection and all Active-X controls shut off by default, Internet Explorer 7 users are protected from attacks from other malicious Web sites. Also, IE7's rewritten URL parser reduces the possibility of buffer overflow attacks.

Computerweekly.com

Full Story :

<http://www.computerweekly.com/Articles/2007/05/25/224065/internet-explorer-security-learning-guide.htm>

❖ EU data-privacy officials probing Google

Concerns over practice of retaining user information for up to two years
BRUSSELS, Belgium - An independent European Union panel has launched an investigation into whether Google Inc.'s Internet search engine abides by European privacy rules.

EU spokesman Pietro Petrucci said Friday that the 28-member panel, which advises the European Commission and EU governments on data protection issues, wants Google to address concerns about the company's practice of storing and retaining user information for up to two years.

"This group has addressed a letter to Google raising a number of questions," Petrucci said, adding that EU Justice Commissioner Franco Frattini was backing the investigation.

msnbc

Full Story :

<http://www.msnbc.msn.com/id/18861687/>

❖ Industry approval for anti-spamming technology

New technology to combat spam and phishing attacks has been approved by the Internet Engineering Task Force (IETF).

The industry group has accepted a draft standard for DomainKeys Identified Mail (DKIM), which uses encrypted digital signatures to validate the identity of an email sender.

The IETF represents internet firms such as Yahoo, Cisco, Sendmail and PGP Corporation. All have pledged to roll out the technology as soon as possible.

Although 90 to 99 per cent of e-mail comes from senders known to the recipient, establishing the identity of a sender is still the main factor in controlling spam because spammers use false or bogus identities.

nvunet

Full Story :

<http://www.vnunet.com/computing/news/2190728/spamming-tool-approval>

New Vulnerabilities Tested in SecureScout

❖ 17760 PHP "php_rand_r()" weaker encryption Vulnerability

A vulnerability has been reported in PHP, which can be exploited by malicious users to decrypt certain data.

The mcrypt_create_iv function in ext/mcrypt/mcrypt.c in PHP before 4.4.7, 5.2.1, and possibly 5.0.x and other PHP 5 versions, calls php_rand_r with an uninitialized seed variable and therefore always generates the same initialization vector (IV), which might allow context-dependent attackers to decrypt certain data more easily because of the guessable encryption keys.

PHP versions 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 are vulnerable to the issue.

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

References:

Original advisory:

<http://blog.php-security.org/archives/80-Watching-the-PHP-CVS.html>

<http://www.fortheloot.com/public/mcrypt.patch>

Other references:

CONFIRM: <http://bugs.php.net/bug.php?id=40999>

CONFIRM: <http://cvs.php.net/viewvc.cgi/php-src/ext/mcrypt/mcrypt.c?r1=1.91.2.3.2.9&r2=1.91.2.3.2.10>

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

BID:23984

URL:<http://www.securityfocus.com/bid/23984>

Product Homepage:

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

CVE Reference: [CVE-2007-2727](https://cve.mitre.org/cve/2007/2727)

❖ 17759 PHP "substr_count" Information disclosure Vulnerability

A vulnerability has been reported in PHP, which can be exploited by malicious users to disclose sensitive information.

The substr_count function in PHP 5.2.1 and earlier allows context-dependent attackers to obtain sensitive information via unspecified vectors, a different affected function than CVE-2007-1375.

PHP versions 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 are vulnerable to the issue.

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

References:

Original advisory:

http://us2.php.net/releases/4_4_7.php

http://us2.php.net/releases/5_2_2.php

Other references:

CONFIRM: http://us2.php.net/releases/5_2_2.php

VIM:20070516 CVE-2007-1375 additional vector?

URL:<http://www.attrition.org/pipermail/vim/2007-May/001621.html>

BID:24012

URL:<http://www.securityfocus.com/bid/24012>

Product Homepage:

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

CVE Reference: [CVE-2007-2748](#)

❖ **17758 PHP "user_filter_factory_create()" code execution Vulnerability**

A vulnerability has been reported in PHP, which can be exploited by malicious users to execute code.

Buffer overflow in the user_filter_factory_create function in PHP before 5.2.2 has unknown impact and local attack vectors.

PHP versions 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 are vulnerable to the issue.

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

References:

Original advisory:

http://us2.php.net/releases/4_4_7.php

http://us2.php.net/releases/5_2_2.php

http://viewcvs.php.net/viewvc.cgi/php-src/ext/standard/user_filters.c?r1=1.31.2.4.2.5&r2=1.31.2.4.2.6

Other references:

MANDRIVA:MDKSA-2007:102

URL:<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:102>

TRUSTIX:2007-0017

URL:<http://www.trustix.org/errata/2007/0017/>

SECUNIA:25191

URL:<http://secunia.com/advisories/25191>

SECUNIA:25255

URL:<http://secunia.com/advisories/25255>

Product Homepage:

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

CVE Reference: [CVE-2007-2511](#)

❖ 17757 PHP "make_http_soap_request()" code execution Vulnerability

A vulnerability has been reported in PHP, which can be exploited by malicious users to execute code.

Buffer overflow in the make_http_soap_request function in PHP before 5.2.2 has unknown impact and remote attack vectors, possibly related to "/" (slash) characters.

PHP versions 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 are vulnerable to the issue.

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

References:

Original advisory:

http://us2.php.net/releases/4_4_7.php

http://us2.php.net/releases/5_2_2.php

http://viewcvs.php.net/viewvc.cgi/php-src/ext/soap/php_http.c?r1=1.77.2.11.2.5&r2=1.77.2.11.2.6

Other references:

DEBIAN:DSA-1295

URL:<http://www.debian.org/security/2007/dsa-1295>

MANDRIVA:MDKSA-2007:102

URL:<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:102>

REDHAT:RHSAs-2007:0348

URL:<https://rhn.redhat.com/errata/RHSA-2007-0348.html>

REDHAT:RHSAs-2007:0355

URL:<http://www.redhat.com/support/errata/RHSA-2007-0355.html>

TRUSTIX:2007-0017

URL:<http://www.trustix.org/errata/2007/0017/>

SECTRACK:1018023

URL:<http://www.securitytracker.com/id?1018023>

SECUNIA:25187

URL:<http://secunia.com/advisories/25187>

SECUNIA:25191

URL:<http://secunia.com/advisories/25191>

SECUNIA:25318

URL:<http://secunia.com/advisories/25318>

SECUNIA:25255

URL:<http://secunia.com/advisories/25255>

Product Homepage:

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

CVE Reference: [CVE-2007-2510](#)

❖ 17756 PHP "ftp_putcmd()" input validation error, data manipulation

Vulnerability

A vulnerability has been reported in PHP, which can be exploited by malicious users to manipulate data.

CRLF injection vulnerability in the ftp_putcmd function in PHP before 4.4.7, and 5.x before 5.2.2 allows remote attackers to inject arbitrary FTP commands via CRLF sequences in the parameters to earlier FTP commands.

PHP versions 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 are vulnerable to the issue.

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

References:

Original advisory:

http://us2.php.net/releases/4_4_7.php

http://us2.php.net/releases/5_2_2.php

Other references:

BUGTRAQ:20070323 CRLF injection in PHP ftp function

URL:<http://www.securityfocus.com/archive/1/archive/1/463596/100/0/threaded>

DEBIAN:DSA-1295

URL:<http://www.debian.org/security/2007/dsa-1295>

MANDRIVA:MDKSA-2007:102

URL:<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:102>

MANDRIVA:MDKSA-2007:103

URL:<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:103>

REDHAT:RHSAs-2007:0348

URL:<https://rhn.redhat.com/errata/RHSA-2007-0348.html>

REDHAT:RHSAs-2007:0349

URL:<http://www.redhat.com/support/errata/RHSA-2007-0349.html>

REDHAT:RHSAs-2007:0355

URL:<http://www.redhat.com/support/errata/RHSA-2007-0355.html>

TRUSTIX:2007-0017

URL:<http://www.trustix.org/errata/2007/0017/>

BID:23818

URL:<http://www.securityfocus.com/bid/23818>

SECTRACK:1018022

URL:<http://www.securitytracker.com/id?1018022>

SECUNIA:25187

URL:<http://secunia.com/advisories/25187>

SECUNIA:25191

URL:<http://secunia.com/advisories/25191>

SECUNIA:25318

URL:<http://secunia.com/advisories/25318>

SECUNIA:25255

URL:<http://secunia.com/advisories/25255>

Product Homepage:

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

CVE Reference: [CVE-2007-2509](https://cve.org/CVERecord?id=CVE-2007-2509)

❖ 17755 PHP libxmlrpc library to allow code execution Vulnerability

A vulnerability has been reported in PHP, which can be exploited by malicious users to execute arbitrary code.

Buffer overflow in the bundled libxmlrpc library in PHP before 4.4.7, and 5.x before 5.2.2, has unknown impact and remote attack vectors.

PHP versions 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 are vulnerable to the issue.

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

References:

Original advisory:

http://us2.php.net/releases/4_4_7.php

http://us2.php.net/releases/5_2_2.php

Other references:

MANDRIVA:MDKSA-2007:102

[URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:102](http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:102)

MANDRIVA:MDKSA-2007:103

[URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:103](http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:103)

REDHAT:RHSAs-2007:0348

[URL:https://rhn.redhat.com/errata/RHSA-2007-0348.html](https://rhn.redhat.com/errata/RHSA-2007-0348.html)

REDHAT:RHSAs-2007:0349

[URL:http://www.redhat.com/support/errata/RHSA-2007-0349.html](http://www.redhat.com/support/errata/RHSA-2007-0349.html)

REDHAT:RHSAs-2007:0355

[URL:http://www.redhat.com/support/errata/RHSA-2007-0355.html](http://www.redhat.com/support/errata/RHSA-2007-0355.html)

TRUSTIX:2007-0017

[URL:http://www.trustix.org/errata/2007/0017/](http://www.trustix.org/errata/2007/0017/)

SECTRACK:1018024

[URL:http://www.securitytracker.com/id?1018024](http://www.securitytracker.com/id?1018024)

SECUNIA:25187

[URL:http://secunia.com/advisories/25187](http://secunia.com/advisories/25187)

SECUNIA:25191

[URL:http://secunia.com/advisories/25191](http://secunia.com/advisories/25191)

SECUNIA:25255

[URL:http://secunia.com/advisories/25255](http://secunia.com/advisories/25255)

Product Homepage:

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

CVE Reference: [CVE-2007-1864](https://cve.mitre.org/cve/2007/1864)

❖ 17754 PHP input validation error in the "mail()" function allows injection of headers via the "To" and "Subject" parameters

A vulnerability has been reported in PHP, which can be exploited by malicious users to manipulate certain data.

CRLF injection vulnerability in the mail function in PHP 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 allows remote attackers to inject arbitrary e-mail headers and possibly conduct spam attacks via a control character immediately following folding of the (1) Subject or (2) To parameter, as demonstrated by a parameter containing a "\r\n\t\n" sequence, related to an increment bug in the SKIP_LONG_HEADER_SEP macro.

PHP versions 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 are vulnerable to the issue.

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

References:

Original advisory:

<http://www.php-security.org/MOPB/MOPB-34-2007.html>

Other references:

CONFIRM: http://us2.php.net/releases/5_2_2.php

DEBIAN:DSA-1282

URL:<http://www.debian.org/security/2007/dsa-1282>

DEBIAN:DSA-1283

URL:<http://www.debian.org/security/2007/dsa-1283>

MANDRIVA:MDKSA-2007:087

URL:<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:087>

MANDRIVA:MDKSA-2007:088

URL:<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:088>

MANDRIVA:MDKSA-2007:089

URL:<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:089>

REDHAT:RHSA-2007:0155

URL:<http://rhn.redhat.com/errata/RHSA-2007-0155.html>

REDHAT:RHSA-2007:0153

URL:<http://www.redhat.com/support/errata/RHSA-2007-0153.html>

REDHAT:RHSA-2007:0162

URL:<http://www.redhat.com/support/errata/RHSA-2007-0162.html>

UBUNTU:USN-455-1

URL:<http://www.ubuntu.com/usn/usn-455-1>

BID:23145

URL:<http://www.securityfocus.com/bid/23145>

SECTrack:1017946

URL:<http://www.securitytracker.com/id?1017946>

SECUNIA:24924

URL:<http://secunia.com/advisories/24924>

SECUNIA:24965

URL:<http://secunia.com/advisories/24965>

SECUNIA:25025

URL:<http://secunia.com/advisories/25025>

SECUNIA:25062

URL:<http://secunia.com/advisories/25062>

SECUNIA:25057

URL:<http://secunia.com/advisories/25057>

SECUNIA:24909

URL:<http://secunia.com/advisories/24909>

Product Homepage:

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

CVE Reference: [CVE-2007-1718](#)

❖ **17753 PHP error in the "mail()" function allows to truncate messages via ASCIIZ bytes**

A vulnerability has been reported in PHP, which can be exploited by malicious users to manipulate certain data.

The mail function in PHP 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 truncates e-mail messages at the first ASCIIZ ('\0') byte, which might allow context-dependent attackers to prevent intended information from being delivered in e-mail messages. NOTE: this issue might be security-relevant in cases when the trailing contents of e-mail messages are important, such as logging information or if the message is expected to be well-formed.

PHP versions 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 are vulnerable to the issue.

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

References:

Original advisory:

<http://www.php-security.org/MOPB/MOPB-33-2007.html>

Other references:

CONFIRM: http://us2.php.net/releases/4_4_7.php

CONFIRM: http://us2.php.net/releases/5_2_2.php

BID:23146

URL:<http://www.securityfocus.com/bid/23146>

Product Homepage:

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

CVE Reference: [CVE-2007-1717](#)

❖ **17752 PHP "bzip2://" wrapper, "safe_mode" and "open_basedir" protection mechanisms bypass**

A vulnerability has been reported in PHP, which can be exploited by malicious users to bypass certain security restrictions.

The compress.bzip2:// URL wrapper provided by the bz2 extension in PHP before 4.4.7, and 5.x before 5.2.2, does not implement safemode or open_basedir checks, which allows remote attackers to read bzip2 archives located outside of the intended directories.

PHP versions 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 are vulnerable to the issue.

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

References:

Original advisory:

<http://www.php-security.org/MOPB/MOPB-21-2007.html>

Other references:

CONFIRM: http://us2.php.net/releases/4_4_7.php

CONFIRM: http://us2.php.net/releases/5_2_2.php

BID:22954

URL:<http://www.securityfocus.com/bid/22954>

Product Homepage:

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

CVE Reference: [CVE-2007-1461](#)

❖ **17751 PHP "zip://" wrapper, "safe_mode" and "open_basedir" protection mechanisms bypass**

A vulnerability has been reported in PHP, which can be exploited by malicious users to bypass certain security restrictions.

The zip:// URL wrapper provided by the PECL zip extension in PHP before 4.4.7, and 5.2.0 and 5.2.1, does not implement safemode or open_basedir checks, which allows remote attackers to read ZIP archives located outside of the intended directories.

PHP versions 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 are vulnerable to the issue.

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

References:

Original advisory:

<http://www.php-security.org/MOPB/MOPB-20-2007.html>

Other references:

CONFIRM: http://us2.php.net/releases/4_4_7.php

CONFIRM: http://us2.php.net/releases/5_2_2.php

BID:22954

URL:<http://www.securityfocus.com/bid/22954>

Product Homepage:

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

CVE Reference: [CVE-2007-1460](#)

New Vulnerabilities found this Week

avast! CAB File Processing Buffer Overflow Vulnerability

"Execution of arbitrary code"

Sergio Alvarez has reported a vulnerability in avast!, which can be exploited by malicious

people to compromise a vulnerable system.

The vulnerability is caused due to an error within the parsing of .CAB files and can be exploited to cause a heap-based buffer overflow via a specially crafted .CAB file.

Successful exploitation may allow execution of arbitrary code.

The vulnerability reportedly affects versions prior to 4.7.766 for servers and 4.7.700 for the Managed Client product.

References:

<http://www.avast.com/eng/avast-4-server-revision-history.html>

<http://www.avast.com/eng/avast-4-server-revision-history.html>

<http://lists.grok.org.uk/pipermail/full-disclosure/2007-May/063566.html>

Cisco CallManager Cross-Site Scripting Vulnerability

“Cross-site scripting attacks”

Marc Ruef and Stefan Friedli have reported a vulnerability in Cisco CallManager, which can be exploited by malicious people to conduct cross-site scripting attacks.

Input passed to parameters in the search form are not properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

Example:

`https://[host]/CCMAdmin/serverlist.asp?findBy=servername&match=begins&pattern=[code]`

The vulnerability is reported in version 4.1. Other versions may also be affected.

References:

<http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2977>

<http://www.cisco.com/warp/public/707/cisco-sr-20070523-ccm.shtml>

PHP "gdPngReadData()" Truncated PNG Data Denial of Service

“Denial of Service”

Xavier Roche has reported a vulnerability in PHP, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to the incorrect use of libpng within the function "gdPngReadData()" in ext/gd/libgd/gd_png.c of the GD extension when processing truncated data. This can be exploited to cause an infinite loop by e.g. tricking an application to process a specially crafted file.

The vulnerability is reported in versions 4.4.7 and 5.2.2. Other versions may also be affected.

References:

http://bugs.libgd.org/?do=details&task_id=86

FreeType TTF Font Parsing Vulnerability

“Denial of Service”

Victor Stinner has reported a vulnerability in FreeType, which can be exploited by malicious people to cause a DoS (Denial of Service) or potentially compromise an application using the library.

The vulnerability is caused due to an error when parsing malformed TTF fonts in src/truetype/ttgload.c and may be exploited when processing a specially crafted TTF font.

The vulnerability is reported in version 2.3.4. Other versions may also be affected.

References:

<http://lists.gnu.org/archive/html/freetype-devel/2007-04/msg00041.html>

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