netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 7

February 16, 2007

Table of Contents

Product Focus

ASN.1 Vulnerability Scanner – The ASN.1 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 MS04-007 that could allow remote code execution.

netVigilance free Single Scanners now support Windows XP Sp2. For a full list and download, go to http://www.netvigilance.com/singlescanners

netvigilance announces support for Delta Reports in SecureScout SP.

This Week in Review

You and your MSSP. Websecurity perspective. Enterprises slow to adopt mobile applications. Hackers to come after corporate data.

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

- **Ensuring a Successful Partnership with Your MSSP**

Securing information assets has become a highly complex function demanding significant investment in process definition, security expertise, systems, and infrastructure. Compounding these challenges, it requires internal alignment between

the various business units, IT organization and security teams to ensure the tensions between availability and security are well balanced. Security is also a 24x7 function, as threats can emerge at anytime.

Generally, there are two approaches to consider for an organization wanting to secure their network. They can do it internally or partner with a managed security services provider (MSSP). Both have their challenges and advantages which each organization should consider based on their circumstance.

An internal approach requires a staff with security expertise, in addition to systems, toolsets, and processes to maintain an organization's security posture around the clock. Organizations that have time and money to implement an internal solution benefit from their ability to fully customize the solution, to integrate internal systems including their ticketing environment and/or patch management systems, and to retain internal security knowledge.

IT-Observer

Full Story :
http://www.it-observer.com/articles.php?id=1306

❖ DNS attack puts Web security in perspective

With more business apps running online, it's time to shore up DoS prevention measures
A few years ago, I had the privilege of seeing some root DNS servers in action at VeriSign's main headquarters. It's something I had wanted to do for over a decade, and I was literally slightly shaking with excitement (yes, I am that big of a geek).
Physical security was high. It took three-factor authentication to get me past the two mantraps and the bomb-blast protected walls. My escort had to use handprint geometry, a PIN, a smart card, and a retinal scan to get me into the inner sanctum.

Turns out VeriSign's DNS root servers at this location are composed of two physically separate, 10-high stacked, 1U pizza-box-style IBM eServers (VeriSign said they tested many different servers, and IBM's gave them the best performance per dollar), running Solaris and Red Hat Linux. Not surprisingly, they don't run BIND and keep things intentionally diverse to protect against a platform-specific attack.

Watching the network lights rapidly blink under millions of transactions per second was a blast. Did I mention I was a geek?

Infoworld

Full Story :
http://www.infoworld.com/article/07/02/16/08OPsecadvise_1.html?source=rss&url=http://www.infoworld.com/article/07/02/16/08OPsecadvise_1.html

❖ 3GSM: Enterprises are uncertain about mobile security

Uncertainty about how to secure mobile phones in the face of increasing threats is slowing enterprise adoption of mobile applications, say experts exhibiting at the 3GSM World Congress in Barcelona.
Over two-thirds of mobile operators in Europe that took part in a survey said that they detected more than 100 incidents involving mobile viruses or mobile spyware in 2006, according to a study by conducted by Informa, for security software developer McAfee.

The number of European operators reporting more than 1 000 such incidents more than doubled in 2006 compared to the previous year, the report says.

IT administrators, uncertain how to protect their users from such attacks, are unwilling to enable mobile access to applications for workers.

ITC world

Full Story :
http://www.ictworld.co.za/EditorialEdit.asp?EditorialID=28202

- **Hackers Turn to Corporate Data**

Among the list of bills introduced with the opening of the U.S. Congress Jan. 5 were two filed by Sen. Dianne Feinstein, D-Calif., aimed at forcing companies to better protect consumer information and publicly report any potential mishandlings.
However, according to a range of IT security researchers, businesses should be just as fearful of having their own valuable data stolen by hackers as they are of losing customer records, as malware writers apparently are ramping efforts to create attacks targeting corporate information.

While researchers have identified myriad viruses aimed at stealing consumer information, there are fewer examples that illustrate this growing focus on stealing business data. Still, experts say there is plenty of evidence that the trend is gaining momentum.

eweek

Full Story :
http://www.eweek.com/article2/0,1759,2095481,00.asp?kc=EWRSS03119TX1K0000594

New Vulnerabilities Tested in SecureScout

- **16419 Vulnerability in Windows Shell Could Allow Elevation of Privilege (MS07-006/928255) (Remote File Checking)**

A privilege elevation vulnerability exists in Windows Shell in the way that the operating system performs detection and registration of new hardware. This vulnerability could allow an authenticated user to take complete control of the system.

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

References:

Original advisory:
MS07-006

http://www.microsoft.com/technet/security/Bulletin/MS07-006.mspx

Other references:
http://www.frsirt.com/english/advisories/2007/0575

CVE Reference: CVE-2007-0211

❖ 16420 Vulnerability in Windows Image Acquisition Service Could Allow Elevation of Privilege (MS07-007/927802) (Remote File Checking)

A privilege elevation vulnerability exists in Windows XP Service Pack 2 in the way that the Window Image Acquisition Service starts applications. This vulnerability could allow a logged on user to take complete control of the system.

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

References:

Original advisory:
MS07-007
http://www.microsoft.com/technet/security/Bulletin/MS07-007.mspx

Other references:
http://secunia.com/advisories/24132/

CVE Reference: CVE-2007-0210

❖ 16421 Vulnerability in HTML Help ActiveX Control Could Allow Remote Code Execution (MS07-008/928843) (Remote File Checking)

A remote code execution vulnerability exists in the HTML Help ActiveX control. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code execution if a user visited that page. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

References:

Original advisory:
MS07-008
http://www.microsoft.com/technet/security/Bulletin/MS07-008.mspx

Other references:
http://secunia.com/advisories/24136/

CVE Reference: CVE-2007-0214

❖ 16422 Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution (MS07-009/927779) (Remote File Checking)

A remote code execution vulnerability exists in the ADODB.Connection ActiveX control that is provided as part of the ActiveX Data Objects (ADO) and that is distributed in MDAC. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

References:

Original advisory:
MS07-009
http://www.microsoft.com/technet/security/Bulletin/MS07-009.mspx

Other references:
MISC: http://www.milw0rm.com/exploits/2629
MISC: http://blogs.technet.com/msrc/archive/2006/10/27/adodb-connection-poc-published.aspx
MISC: http://research.eeye.com/html/alerts/zeroday/20061027.html
CERT-VN:VU#589272
URL:http://www.kb.cert.org/vuls/id/589272
BID:20704
URL:http://www.securityfocus.com/bid/20704
SECTRACK:1017127
URL:http://securitytracker.com/id?1017127
XF:ie-adodbconnection-Code-Execution(29837)
URL:http://xforce.iss.net/xforce/xfdb/29837

CVE Reference: CVE-2006-5559

❖ 16424 Vulnerability in Microsoft OLE Dialog Could Allow Remote Code Execution (MS07-011/926436) (Remote File Checking)

A remote code execution vulnerability exists in the OLE Dialog component provided with Microsoft Windows. An attacker could attempt to exploit this vulnerability when a user interacts with a malformed embedded OLE object within a Rich Text Format (RTF) file.

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

References:

Original advisory:
MS07-011
http://www.microsoft.com/technet/security/Bulletin/MS07-011.mspx

Other references:
http://secunia.com/advisories/24147/
http://www.frsirt.com/english/advisories/2007/0580

CVE Reference: CVE-2007-0026

❖ 16425 Vulnerability in Microsoft MFC Could Allow Remote Code Execution (MS07-012/924667) (Remote File Checking)

A remote code execution vulnerability exists in the MFC component provided with Microsoft Windows and Visual Studio. An attacker could exploit this vulnerability when a user interacts with a malformed embedded OLE object within a Rich Text Format (RTF) file.

If a user were 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. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative rights.

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

References:

Original advisory:
MS07-012
http://www.microsoft.com/technet/security/Bulletin/MS07-012.mspx

Other references:
http://secunia.com/advisories/24150/
http://www.frsirt.com/english/advisories/2007/0581

CVE Reference: CVE-2007-0025

❖ 16426 Vulnerability in Microsoft RichEdit Could Allow Remote Code Execution (MS07-013/918118) (Remote File Checking)

A remote code execution vulnerability exists in the RichEdit components provided with Microsoft Windows and Microsoft Office. An attacker could exploit this vulnerability when a user interacts with a malformed embedded OLE object within a Rich Text Format (RTF) file.

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. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

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

References:

Original advisory:

MS07-013
http://www.microsoft.com/technet/security/Bulletin/MS07-013.mspx

Other references:
http://secunia.com/advisories/24152/
http://www.frsirt.com/english/advisories/2007/0582

CVE Reference: CVE-2006-1311

❖ 16427 Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (MS07-014/929434) (Remote File Checking)

Word Malformed String Vulnerability - CVE-2006-5994:

A remote code execution vulnerability exists in the way Microsoft Word handles Word files with a specially crafted string. Such a specially crafted file might be included as an e-mail attachment or hosted on a malicious Web site. An attacker could exploit the vulnerability by constructing a specially crafted Word file that could allow remote code execution.

Word Malformed Data Structures Vulnerability - CVE-2006-6456:

A remote code execution vulnerability exists in the way Microsoft Word handles Word files with a specially crafted data structure. Such a specially crafted file might be included as an e-mail attachment or hosted on a malicious Web site. An attacker could exploit the vulnerability by constructing a specially crafted Word file that could allow remote code execution. Viewing or previewing a malformed e-mail message in an affected version of Outlook could not lead to exploitation of this vulnerability.

Word Count Vulnerability – CVE-2006-6561:

A remote code execution vulnerability exists in Microsoft Word. An attacker could exploit this vulnerability when Word parses a file and processes an unchecked count. Such a specially crafted file might be included as an e-mail attachment or hosted on a malicious Web site. An attacker could exploit the vulnerability by constructing a specially crafted Word file that could allow remote code execution. Viewing or previewing a malformed e-mail message in an affected version of Outlook could not lead to exploitation of this vulnerability.

Word Macro Vulnerability – CVE-2007-0208:

A remote code execution vulnerability exists in Microsoft Word. 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Word Malformed Drawing Object Vulnerability - CVE-2007-0209:

A remote code execution vulnerability exists in Microsoft Word. An attacker could exploit this vulnerability when Word parses a file and processes a malformed drawing object. Such a specially crafted file might be included as an e-mail attachment or hosted on a malicious Web site. An attacker could exploit the vulnerability by

constructing a specially crafted Word file that could allow remote code execution.

Word Malformed Function Vulnerability - CVE-2007-0515:

A remote code execution vulnerability exists in Microsoft Word. An attacker could exploit this vulnerability when Word parses a file and processes a malformed function. Such a specially crafted file might be included as an e-mail attachment or hosted on a malicious web site. Viewing or previewing a malformed e-mail message in an affected version of Outlook could not lead to exploitation of this vulnerability. An attacker could exploit the vulnerability by constructing a specially crafted Word file that could allow remote code execution.

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

References:

CVE Reference: CVE-2006-5994
CVE-2006-6456
CVE-2006-6561
CVE-2007-0208
CVE-2007-0209
CVE-2007-0515

❖ 16428 Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (MS07-015/932554) (Remote File Checking)

PowerPoint Malformed Record Memory Corruption Vulnerability - CVE-2006-3877:

A remote code execution vulnerability exists in PowerPoint and could be exploited when PowerPoint opened a specially crafted file. Such a file might be included in an e-mail attachment or hosted on a malicious web site. An attacker could exploit the vulnerability by constructing a specially crafted PowerPoint file that could allow remote code execution.

If a user were 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. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

Excel Malformed Record Vulnerability - CVE-2007-0671:

A remote code execution vulnerability exists in Excel and could be exploited when Excel opened a specially crafted file. Such a file might be included in an e-mail attachment or hosted on a malicious web site. An attacker could exploit the vulnerability by constructing a specially crafted Excel file that could allow remote code execution.

If a user were 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. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

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

References:

Original advisory:
MS07-015
http://www.microsoft.com/technet/security/Bulletin/MS07-015.mspx

Other references:
* HP:HPSBST02161
* URL:http://www.securityfocus.com/archive/1/archive/1/449179/100/0/threaded
* HP:SSRT061264
* MS:MS06-058
* URL:http://www.microsoft.com/technet/security/Bulletin/MS06-058.mspx
* MS:MS07-015
* URL:http://www.microsoft.com/technet/security/Bulletin/MS07-015.mspx
* CERT-VN:VU#205948
* URL:http://www.kb.cert.org/vuls/id/205948
* BID:20325
* URL:http://www.securityfocus.com/bid/20325
* FRSIRT:ADV-2006-3977
* URL:http://www.frsirt.com/english/advisories/2006/3977
* OSVDB:29448
* URL:http://www.osvdb.org/29448
* OVAL:oval:org.mitre.oval:def:220
* URL:http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:220
* SECTRACK:1017030
* URL:http://securitytracker.com/id?1017030
* MISC: http://vil.nai.com/vil/content/v_141393.htm
* MISC: http://www.avertlabs.com/research/blog/?p=191
* CONFIRM: http://www.microsoft.com/technet/security/advisory/932553.mspx
* CERT-VN:VU#613740
* URL:http://www.kb.cert.org/vuls/id/613740
* BID:22383
* URL:http://www.securityfocus.com/bid/22383
* FRSIRT:ADV-2007-0463
* URL:http://www.frsirt.com/english/advisories/2007/0463
* SECTRACK:1017584
* URL:http://securitytracker.com/id?1017584
* SECUNIA:24008
* URL:http://secunia.com/advisories/24008
* XF:office-unspecified-code-execution(32178)
* URL:http://xforce.iss.net/xforce/xfdb/32178

CVE Reference: CVE-2006-3877

❖ **16429 Cumulative Security Update for Internet Explorer (MS07-016/928090) (Remote File Checking)**

COM Object Instantiation Memory Corruption Vulnerability - CVE-2006-4697:

A remote code execution vulnerability exists in the way Internet Explorer instantiates COM objects that are not intended to be instantiated in Internet Explorer. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code execution if a user viewed the Web page. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

COM Object Instantiation Memory Corruption Vulnerability - CVE-2007-0219:

A remote code execution vulnerability exists in the way Internet Explorer instantiates COM objects that are not intended to be instantiated in Internet Explorer. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code execution if a user viewed the Web page. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

FTP Server Response Parsing Memory Corruption Vulnerability - CVE-2007-0217:

A remote code execution vulnerability exists in the way Internet Explorer interprets certain responses from FTP servers. An attacker could exploit the vulnerability by sending specially crafted FTP responses in an FTP session to the FTP client included in Internet Explorer. An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

Original advisory:
MS07-016
http://www.microsoft.com/technet/security/Bulletin/MS07-016.mspx

Other references:
http://www.frsirt.com/english/advisories/2007/0584
http://secunia.com/advisories/24156/

CVE Reference: CVE-2006-4697
CVE-2007-0219
CVE-2007-0219

New Vulnerabilities found this Week

Internet Explorer Multiple Vulnerabilities
"Execution of arbitrary code"

Some vulnerabilities have been reported in Internet Explorer, which can be exploited by malicious people to compromise a user's system.

1) An error within the instantiation of COM objects (Imjpcksid.dll and Imjpskdic.dll) not

intended to be instantiated in Internet Explorer can be exploited to cause a memory corruption.

2) Another error within the instantiation of COM objects (Msb1fren.dll, Htmlmm.ocx, and Blnmgrps.dll) not intended to be instantiated in Internet Explorer can be exploited to cause a memory corruption.

3) An off-by-one error in wininet.dll within the parsing of FTP server responses can be exploited to cause memory corruption via specially crafted responses sent to the FTP client in Internet Explorer.

Successful exploitation of the vulnerabilities allows execution of arbitrary code.

References:
http://www.microsoft.com/technet/security/Bulletin/MS07-016.mspx
http://descriptions.securescout.com/tc/16429

Microsoft RichEdit OLE Dialog Memory Corruption Vulnerability
"Memory corruption"

A vulnerability has been reported in Microsoft Windows and Microsoft Office, which can be exploited by malicious people to compromise a users system.

The vulnerability is caused due to an error in RichEdit components handling of OLE objects in RTF (Rich Text Format) files. This can be exploited to cause a memory corruption by e.g. tricking a user into opening a malicious RTF document using a Microsoft Office application and interact with a specially crafted, embedded OLE object.

References:
http://www.microsoft.com/technet/security/Bulletin/MS07-013.mspx
http://descriptions.securescout.com/tc/16426

Microsoft MFC OLE Dialog Memory Corruption Vulnerability
"Execution of arbitrary code"

A vulnerability has been reported in Microsoft Windows and Visual Studio, which can be exploited by malicious people to compromise a users system.

The vulnerability is caused due to a memory corruption in the MFC component when handling OLE objects in Rich Text Format (RTF) files. This can be exploited by e.g. tricking a user into opening a malicious RTF document using Wordpad and interact with a specially crafted embedded OLE object.

Successful exploitation allows execution of arbitrary code.

References:
http://www.microsoft.com/technet/security/Bulletin/MS07-012.mspx
http://descriptions.securescout.com/tc/16425

Microsoft Windows OLE Dialog Memory Corruption Vulnerability

“Execution of arbitrary code”

A vulnerability has been reported in Microsoft Windows, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an error in Windows OLE Dialog components handling of OLE objects in RTF (Rich Text Format) files. This can be exploited to cause a memory corruption by e.g. tricking a user into opening a malicious RTF document using Wordpad and interact with a specially crafted embedded OLE object.

Successful exploitation allows execution of arbitrary code.

References:
http://www.microsoft.com/technet/security/Bulletin/MS07-011.mspx
http://descriptions.securescout.com/tc/16424

Microsoft Windows HTML Help ActiveX Control Vulnerability
“Execution of arbitrary code”

A vulnerability has been reported in Microsoft Windows, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to certain parameters not being properly initialised by the HTML ActiveX control (Hhctrl.ocx) when handling certain methods.

Successful exploitation allows execution of arbitrary code when a user e.g. visits a malicious website.

NOTE: Other unspecified issues discovered internally by Microsoft have also been reported.

References:
http://www.microsoft.com/technet/security/Bulletin/MS07-008.mspx
http://descriptions.securescout.com/tc/16421

Microsoft Windows Image Aquisition Service Privilege Escalation
“Execute code with escalated privileges”

A vulnerability has been reported in Microsoft Windows XP, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to an unchecked buffer in the Windows Image Acquisition service and can be exploited to execute code with escalated privileges.

References:
http://www.microsoft.com/technet/security/Bulletin/MS07-007.mspx
http://descriptions.securescout.com/tc/16420

Microsoft Step-by-Step Interactive Training Bookmark Link File Buffer Overflow
“Execution of arbitrary code”

A vulnerability has been reported in Microsoft Step-by-Step Interactive Training, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the handling of Step-by-Step Interactive Training bookmark link files (.cbo, .cbl, .cbm). This can be exploited to cause a buffer overflow via e.g. a specially crafted web page.

Successful exploitation allows execution of arbitrary code.

References:
http://www.microsoft.com/technet/security/Bulletin/MS07-005.mspx

Microsoft Windows Shell Privilege Escalation Vulnerability
"Gain escalated privileges"

A vulnerability has been reported in Microsoft Windows, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to an unspecified error in the Windows Shell detection and registration of new hardware.

Successful exploitation allows execution of code with escalated privileges.

References:
http://www.microsoft.com/technet/security/Bulletin/MS07-006.mspx
http://descriptions.securescout.com/tc/16419

Microsoft Malware Protection Engine PDF File Parsing Vulnerability
"Execution of arbitrary code"

A vulnerability has been reported in Microsoft Malware Protection Engine, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an integer overflow error when parsing PDF (Portable Document Format) files. This can be exploited to cause a buffer overflow when a specially crafted PDF file is scanned.

Successful exploitation allows execution of arbitrary code.

References:
http://www.microsoft.com/technet/security/Bulletin/MS07-010.mspx

Microsoft MDAC ADODB.Connection ActiveX Control Vulnerability
"Execution of arbitrary code"

Yag Kohha has reported a vulnerability in Microsoft Data Access Components, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an error in the ADODB.Connection ActiveX control when handling the "Execute()" method. This can be exploited to cause a memory corruption by passing specially crafted parameters to the method.

Successful exploitation may allow execution of arbitrary code when a user e.g. visits a malicious website.

References:
http://www.microsoft.com/technet/security/Bulletin/MS07-009.mspx
http://descriptions.securescout.com/tc/16422

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