

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

[RPC DCOM Vulnerabilities Scanner](#) - The S4 RPC DCOM Vulnerabilities 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 RPC DCOM flaws (MS03-026 and MS03-039).

Download Here:

<http://www.netvigilance.com/productdownloads?productname=rpcdcomvulnerabilityesscanner>

This Week in Review

PCI Security Standards discussed at House hearing. Security during the crisis. A story from real life. Vendors found cloud security alliance.

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

• PCI security standard gets ripped at House hearing

April 1, 2009 (Computerworld) The PCI standard, long touted as one of the private sector's best attempts to regulate itself on data security, is increasingly showing signs of coming apart at the seams.

The hearing, held by a subcommittee of the House Committee on Homeland Security, also highlighted the longstanding bitter divide between retailers on one side and banks and credit card companies on the other over the role that the latter organizations should play in protecting card data.

Much of PCI's limitations have to do with the static nature of the standard's requirements, according to Clarke, who said the rules are ineffective at dealing with the highly dynamic security threats that retailers and other merchants now face.

Computerworld

Full Story :

• Turning tough times to your advantage

April 1, 2009 (Network World) Although vendor-written, this contributed piece does not advocate a position that is particular to the author's employer and has been edited and approved by Network World Editor in Chief, John Dix.

To capitalize on the moment, security groups need to reassess their approach, add visibility and transform security's very role.

Risk is further exacerbated by the fact that, since the last economic crisis of this magnitude, companies have become far more reliant on information technology systems, which are now highly complex and essential to sound operations.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9130900&source=rss_topic1

• Diary of a Data Breach Investigation

April 1, 2009 (CSO) Monday

It appears that we have been passing sensitive information to them over the Internet. This sensitive information included data, such as customer names, addresses and credit card information. Because we are a public company, there are many regulatory guidelines that we have to follow like Sarbanes-Oxley (SOX) and the Payment Card Industry's (PCI) data security standard.

Unfortunately for us, it was six months of information totaling over a terabyte.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9130862&source=rss_topic1

• Cloud Security Alliance formed to promote best practices

March 31, 2009 (Network World) A group calling itself the Cloud Security Alliance announced its formation Tuesday, with eBay and ING as founding members.

The on-demand cloud computing model is putting new demand on security, according to statements from Dave Cullinane, CISO at eBay. "The very nature of how businesses use information technology is being transformed by the on-demand cloud computing model," he said. "It is imperative that information security leaders are engaged at this early stage to help assure that the rapid adoption of cloud computing builds in information security best practices without impeding the business."

Chris Hoff, technical advisor to the Cloud Security Alliance, says the group, which includes a mix of user companies and vendors (PGP, Qualys and vScaler are among those announced) wants to sort out issues coming up in the cloud computing environment today.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9130884&source=rss_topic1

• Owning your own data

April 2, 2009 (Network World) The idea of you "owning" the data about yourself is both emotionally and intellectually appealing. This data, which ranges from the critical (your medical and financial records) to the theoretically trivial (what you buy and search for, and which Web sites you visit) defines, quantifies and describes your preferences, resources, habits and health. It is a proxy for you. It is also what every marketer in the entire commercial universe wants to get their hands on.

This data might be high grade (for example, your tax returns and medical records are in-depth, detailed and specific), or low grade (such as your Google searches and your click stream as you navigate Amazon). But whatever the source or the quality, that data has value and it is guaranteed that someone, somewhere, considers even the smallest part of it valuable and worth exploiting.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9131020&source=rss_topic1

New Vulnerabilities Tested in SecureScout

• 18321 QuickTime handling of RTSP URLs buffer overflow (Remote File Checking)

A heap buffer overflow exists in QuickTime's handling of RTSP URLs. Accessing a maliciously crafted RTSP URL may lead to an unexpected application termination or arbitrary code execution. This update addresses the issue by performing additional validation of RTSP URLs.

The issue has been fixed in version 7.6.

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

References:

- * CONFIRM:
<http://support.apple.com/kb/HT3403>
- * APPLE: APPLE-SA-2009-01-21
<http://lists.apple.com/archives/security-announce/2009/Jan/msg00000.html>
- * CERT: TA09-022A
<http://www.us-cert.gov/cas/techalerts/TA09-022A.html>
- * BID: 33385
<http://www.securityfocus.com/bid/33385>
- * OVAL: oval:org.mitre.oval:def:6135
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6135>
- * NETVIGILANCE-UNKNOWN: ADV-2009-0212
<http://www.frsirt.com/english/advisories/2009/0212>
- * SECUNIA: 33632
<http://secunia.com/advisories/33632>
- * XF: quicktime-rtspurl-bo(48154)
<http://xforce.iss.net/xforce/xfdb/48154>

CVE Reference:

CVE-2009-0001 (cve.mitre.org, nvd.nist.gov)

• 18322 QuickTime handling of THKD atoms in QTVR movie files buffer overflow (Remote File Checking)

A heap buffer overflow exists in QuickTime's handling of THKD atoms in QTVR (QuickTime Virtual Reality) movie files. Viewing a maliciously crafted QTVR file may lead to an unexpected application termination or arbitrary code execution. This update addresses the issue through improved bounds checking.

The issue has been fixed in version 7.6.

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

References:

- * BUGTRAQ: 20090121 ZDI-09-005: Apple QuickTime VR Track Header Atom Heap Corruption Vulnerability
<http://archives.neohapsis.com/archives/bugtraq/2009-01/0210.html>
- * MISC:
<http://www.zerodayinitiative.com/advisories/ZDI-09-005/>
- * CONFIRM:
<http://support.apple.com/kb/HT3403>
- * APPLE: APPLE-SA-2009-01-21
<http://lists.apple.com/archives/security-announce/2009/Jan/msg00000.html>
- * CERT: TA09-022A
<http://www.us-cert.gov/cas/techalerts/TA09-022A.html>
- * BID: 33384
<http://www.securityfocus.com/bid/33384>
- * OVAL: oval:org.mitre.oval:def:5646
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5646>
- * NETVIGILANCE-UNKNOWN: ADV-2009-0212
<http://www.frsirt.com/english/advisories/2009/0212>
- * OSVDB: 51525
<http://osvdb.org/51525>
- * SECUNIA: 33632
<http://secunia.com/advisories/33632>

CVE Reference:

CVE-2009-0002 (cve.mitre.org, nvd.nist.gov)

• **18323 QuickTime handling of AVI movie file buffer overflow (Remote File Checking)**

A heap buffer overflow may occur while processing an AVI movie file. Opening a maliciously crafted AVI movie file may lead to an unexpected application termination or arbitrary code execution. This update addresses the issue through improved bounds checking.

The issue has been fixed in version 7.6.

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

References:

- * MISC:
<http://www.zerodayinitiative.com/advisories/ZDI-09-006/>
- * CONFIRM:
<http://support.apple.com/kb/HT3403>
- * APPLE: APPLE-SA-2009-01-21
<http://lists.apple.com/archives/security-announce/2009/Jan/msg00000.html>
- * CERT: TA09-022A
<http://www.us-cert.gov/cas/techalerts/TA09-022A.html>
- * BID: 33387
<http://www.securityfocus.com/bid/33387>
- * OVAL: oval:org.mitre.oval:def:6218
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6218>
- * NETVIGILANCE-UNKNOWN: ADV-2009-0212
<http://www.frsirt.com/english/advisories/2009/0212>
- * OSVDB: 51526
<http://osvdb.org/51526>
- * SECUNIA: 33632
<http://secunia.com/advisories/33632>

CVE Reference:

CVE-2009-0003 (cve.mitre.org, nvd.nist.gov)

• **18324 QuickTime handling of MPEG-2 video files with MP3 audio content buffer overflow (Remote File Checking)**

A buffer overflow exists in the handling of MPEG-2 video files with MP3 audio content. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution. This update addresses the issue through improved bounds checking.

The issue has been fixed in version 7.6.

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

References:

- * CONFIRM:
<http://support.apple.com/kb/HT3403>
- * APPLE: APPLE-SA-2009-01-21
<http://lists.apple.com/archives/security-announce/2009/Jan/msg00000.html>
- * CERT: TA09-022A
<http://www.us-cert.gov/cas/techalerts/TA09-022A.html>
- * OVAL: oval:org.mitre.oval:def:6211
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6211>
- * NETVIGILANCE-UNKNOWN: ADV-2009-0212
<http://www.frsirt.com/english/advisories/2009/0212>
- * SECUNIA: 33632
<http://secunia.com/advisories/33632>
- * XF: quicktime-mpeg2-bo(48157)
<http://xforce.iss.net/xforce/xfdb/48157>

CVE Reference:

CVE-2009-0004 (cve.mitre.org, nvd.nist.gov)

• **18325 QuickTime handling of H.263 encoded movie files memory corruption (Remote File Checking)**

A memory corruption exists in QuickTime's handling of H.263 encoded movie files. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution. This update addresses the

issue by performing additional validation of H.263 encoded movie files.

The issue has been fixed in version 7.6.

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

References:

- * CONFIRM:
<http://support.apple.com/kb/HT3403>
- * APPLE: APPLE-SA-2009-01-21
<http://lists.apple.com/archives/security-announce/2009/Jan/msg00000.html>
- * CERT: TA09-022A
<http://www.us-cert.gov/cas/techalerts/TA09-022A.html>
- * BID: 33386
<http://www.securityfocus.com/bid/33386>
- * OVAL: oval:org.mitre.oval:def:6187
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6187>
- * NETVIGILANCE-UNKNOWN: ADV-2009-0212
<http://www.frsirt.com/english/advisories/2009/0212>
- * SECUNIA: 33632
<http://secunia.com/advisories/33632>
- * XF: quicktime-h263-movie-code-execution(48158)
<http://xforce.iss.net/xforce/xfdb/48158>

CVE Reference:

CVE-2009-0005 (cve.mitre.org, nvd.nist.gov)

• 18326 QuickTime handling of Cinepak encoded movie files buffer overflow (Remote File Checking)

A signedness issue exists in QuickTime's handling of Cinepak encoded movie files, which may result in a heap buffer overflow. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution. This update addresses the issue by performing additional validation of movie files.

The issue has been fixed in version 7.6.

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

References:

- * BUGTRAQ: 20090121 ZDI-09-007: Apple QuickTime Cinepak Codec MDAT Heap Corruption Vulnerability
<http://archives.neohapsis.com/archives/bugtraq/2009-01/0215.html>
- * BUGTRAQ: 20090124 Re: ZDI-09-007: Apple QuickTime Cinepak Codec MDAT Heap Corruption Vulnerability
<http://www.securityfocus.com/archive/1/archive/1/500391/100/0/threaded>
- * MISC:
<http://www.zerodayinitiative.com/advisories/ZDI-09-007/>
- * CONFIRM:
<http://support.apple.com/kb/HT3403>
- * APPLE: APPLE-SA-2009-01-21
<http://lists.apple.com/archives/security-announce/2009/Jan/msg00000.html>
- * CERT: TA09-022A
<http://www.us-cert.gov/cas/techalerts/TA09-022A.html>
- * BID: 33388
<http://www.securityfocus.com/bid/33388>
- * OVAL: oval:org.mitre.oval:def:6153
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6153>
- * NETVIGILANCE-UNKNOWN: ADV-2009-0212
<http://www.frsirt.com/english/advisories/2009/0212>
- * OSVDB: 51529
<http://osvdb.org/51529>
- * SECUNIA: 33632
<http://secunia.com/advisories/33632>

CVE Reference:

CVE-2009-0006 (cve.mitre.org, nvd.nist.gov)

• 18327 QuickTime handling of jpeg atoms in QuickTime movie files buffer overflow (Remote File Checking)

A heap buffer overflow exists in QuickTime's handling of jpeg atoms in QuickTime movie files. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution. This update

addresses the issue through improved bounds checking.

The issue has been fixed in version 7.6.

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

References:

- * MISC:
<http://www.zerodayinitiative.com/advisories/ZDI-09-008/>
- * CONFIRM:
<http://support.apple.com/kb/HT3403>
- * APPLE: APPLE-SA-2009-01-21
<http://lists.apple.com/archives/security-announce/2009/Jan/msg00000.html>
- * CERT: TA09-022A
<http://www.us-cert.gov/cas/techalerts/TA09-022A.html>
- * BID: 33390
<http://www.securityfocus.com/bid/33390>
- * OVAL: oval:org.mitre.oval:def:6132
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6132>
- * NETVIGILANCE-UNKNOWN: ADV-2009-0212
<http://www.frsirt.com/english/advisories/2009/0212>
- * OSVDB: 51530
<http://osvdb.org/51530>
- * SECUNIA: 33632
<http://secunia.com/advisories/33632>

CVE Reference:

CVE-2009-0007 (cve.mitre.org, nvd.nist.gov)

• 18328 QuickTime MPEG-2 Playback Component for Windows input validation issue (Remote File Checking)

An input validation issue exists in the QuickTime MPEG-2 Playback Component for Windows. Accessing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution. This update addresses the issue by performing additional validation of MPEG-2 files. This issue does not affect systems running Mac OS X. Credit to Richard Lemon of Code Lemon for reporting this issue.

The QuickTime MPEG-2 Playback Component is not installed by default, and is provided separately from QuickTime.

The issue has been fixed in version 7.6.

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

References:

- * CONFIRM:
<http://support.apple.com/kb/HT3404>
- * APPLE: APPLE-SA-2009-01-21
<http://lists.apple.com/archives/security-announce//2009/Jan/msg00001.html>
- * BID: 33393
<http://www.securityfocus.com/bid/33393>
- * OVAL: oval:org.mitre.oval:def:5974
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5974>
- * NETVIGILANCE-UNKNOWN: ADV-2009-0211
<http://www.frsirt.com/english/advisories/2009/0211>
- * SECTrack: 1021621
<http://www.securitytracker.com/id?1021621>
- * SECUNIA: 33642
<http://secunia.com/advisories/33642>
- * XF: quicktime-mpeg2playback-code-execution(48162)
<http://xforce.iss.net/xforce/xfdb/48162>

CVE Reference:

CVE-2009-0008 (cve.mitre.org, nvd.nist.gov)

• 18329 QuickTime MOV file with "long arguments" buffer overflow (Remote File Checking)

Stack-based buffer overflow in Apple QuickTime Player 7.5.5 and iTunes 8.0.2.20 allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a MOV file with "long arguments", related to an "off by one overflow."

The issue has been fixed in version 7.6.

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

References:

- * MILWORM: 7296
<http://www.milw0rm.com/exploits/7296>
- * BID: 32540
<http://www.securityfocus.com/bid/32540>
- * SREASON: 4704
<http://securityreason.com/securityalert/4704>
- * XF: apple-quicktime-itunes-mov-bo(46984)
<http://xforce.iss.net/xforce/xfdb/46984>

CVE Reference:

CVE-2008-5406 (cve.mitre.org, nvd.nist.gov)

• 18330 QuickTime long type attribute in a quicktime tag buffer overflow (Remote File Checking)

Buffer overflow in Apple QuickTime 7.5.5 and iTunes 8.0 allows remote attackers to cause a denial of service (browser crash) or possibly execute arbitrary code via a long type attribute in a quicktime tag on a web page or embedded in a .mp4 or .mov file, possibly related to the Check_stack_cookie function and an off-by-one error that leads to a heap-based buffer overflow.

The issue has been fixed in version 7.6.

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

References:

- * MILWORM: 6471
<http://www.milw0rm.com/exploits/6471>
- * BID: 31212
<http://www.securityfocus.com/bid/31212>
- * OVAL: oval:org.mitre.oval:def:5936
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5936>
- * OVAL: oval:org.mitre.oval:def:6113
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6113>
- * SREASON: 4270
<http://securityreason.com/securityalert/4270>
- * XF: quicktime-itunes-checkstackcookie-bo(45311)
<http://xforce.iss.net/xforce/xfdb/45311>

CVE Reference:

CVE-2008-4116 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2007-6722 Microsoft CVSS 2.0 Score = 10.0

Vidalia bundle before 0.1.2.18, when running on Windows and Mac OS X, installs Privoxy with a configuration file (config.txt or config) that contains insecure (1) enable-remote-toggle and (2) enable-edit-actions settings, which allows remote attackers to bypass intended access restrictions and modify configuration.

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

References:

MLIST: <http://archives.seul.org/or/talk/Oct-2007/msg00291.html>

CVE Reference: [CVE-2007-6722](http://cve.mitre.org/cve/2007/6722)

• CVE-2007-6724 Microsoft CVSS 2.0 Score = 10.0

Vidalia bundle before 0.1.2.18, when running on Windows and Mac OS X, installs Privoxy with a configuration file (config.txt or config) that contains an insecure enable-remote-http-toggle setting, which allows remote attackers to bypass intended access restrictions and modify configuration.

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

References:

MLIST: <http://archives.seul.org/or/talk/Oct-2007/msg00291.html>

CVE Reference: [CVE-2007-6724](#)

• CVE-2009-1216 Microsoft CVSS 2.0 Score = 10.0

Multiple unspecified vulnerabilities in (1) unlzh.c and (2) unpack.c in the gzip libraries in Microsoft Windows Server 2008, Windows Services for UNIX 3.0 and 3.5, and the Subsystem for UNIX-based Applications (SUA); as used in gunzip, gzip, pack, pcat, and unpack 7.x before 7.0.1701.48, 8.x before 8.0.1969.62, and 9.x before 9.0.3790.2076; allow remote attackers to execute arbitrary code via unknown vectors.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/49435>

VUPEN: <http://www.vupen.com/english/advisories/2009/0849>

MSKB: <http://support.microsoft.com/kb/953602>

SECTrack: <http://securitytracker.com/id?1021937>

SECUNIA: <http://secunia.com/advisories/34428>

CVE Reference: [CVE-2009-1216](#)

• CVE-2009-1217 Microsoft CVSS 2.0 Score = 9.3

Off-by-one error in the GpFont::SetData function in gdiplus.dll in Microsoft GDI+ on Windows XP allows remote attackers to cause a denial of service (stack corruption and application termination) via a crafted EMF file that triggers an integer overflow, as demonstrated by voltage-exploit.emf, aka the "Microsoft GdiPlus EMF GpFont.SetData integer overflow."

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/49438>

VUPEN: <http://www.vupen.com/english/advisories/2009/0832>

CONFIRM: <http://blogs.technet.com/srd/archive/2009/03/26/new-emf-gdiplus-dll-crash-not-exploitable-for-code-execution.aspx>

MISC: <http://bl4cksecurity.blogspot.com/2009/03/microsoft-gdiplus-emf-gpfontsetdata.html>

CVE Reference: [CVE-2009-1217](#)

• CVE-2009-1233 Microsoft CVSS 2.0 Score = 7.1

Apple Safari 3.2.2 and 4 Beta on Windows allows remote attackers to cause a denial of service (application crash) via an XML document containing many nested A elements.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/49527>

BID: <http://www.securityfocus.com/bid/34318>

MILWORM: <http://www.milw0rm.com/exploits/8325>

CVE Reference: [CVE-2009-1233](#)

• CVE-2009-1172 IBM CVSS 2.0 Score = 10.0

The JAX-RPC WS-Security runtime in the Web Services Security component in IBM WebSphere Application Server (WAS) 6.1 before 6.1.0.23 and 7.0 before 7.0.0.3, when APAR PK41002 is installed, does not properly validate UsernameToken objects, which has unknown impact and attack vectors.

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

References:

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27014463>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27007951>

SECUNIA: <http://secunia.com/advisories/34461>

SECUNIA: <http://secunia.com/advisories/34131>

CVE Reference: [CVE-2009-1172](#)

• CVE-2009-1174 IBM CVSS 2.0 Score = 10.0

The Web Services Security component in IBM WebSphere Application Server (WAS) 7.0 before 7.0.0.3 has an unspecified "security problem" in the XML digital-signature specification, which has unknown impact and attack vectors.

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

References:

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27014463>

SECUNIA: <http://secunia.com/advisories/34461>

CVE Reference: [CVE-2009-1174](#)

• CVE-2009-1178 IBM CVSS 2.0 Score = 10.0

Unspecified vulnerability in the server in IBM Tivoli Storage Manager (TSM) 5.3.x before 5.3.2 and 6.x before 6.1 has unknown impact and attack vectors related to the "admin command line."

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

References:

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21246076>

VUPEN: <http://www.vupen.com/english/advisories/2009/0881>

BID: <http://www.securityfocus.com/bid/34285>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21375360>

SECTRAK: <http://securitytracker.com/id?1021945>

SECUNIA: <http://secunia.com/advisories/34498>

CVE Reference: [CVE-2009-1178](#)

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