

## Table of Contents

[Product Focus](#)

[This Week in Review](#)

[Top Security News Stories this Week](#)

[New Vulnerabilities Tested in SecureScout](#)

[New Vulnerabilities found this Week](#)

---

## Product Focus

[Apache Chunked Vulnerability Scanner](#) - The S4 Apache Chunked Vulnerability Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the Apache Chunked Encoding buffer overflow.

Download Here:

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

## This Week in Review

A way to simpler PCI compliance. Secure business data in the Cloud. Her-you-have under investigation. Application security problems are huge.

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

### • PCI Council: P2PE simplifies PCI DSS compliance

The group responsible for managing payment security rules plans to release two new guidance documents early next month assessing the impact of emerging data security technologies on payment card security.

One of the documents will focus on point-to-point encryption (P2PE), also commonly known as end-to-end encryption, an emerging technology used to mask cardholder data from point-of-swipe through processing. Properly implemented P2PE will allow merchants to reduce their scope in complying with the Payment Card Industry Data Security Standard (PCI DSS), Troy Leach, chief standards architect for the PCI Security Standards Council (SSC) said during a presentation at the PCI North American Community Meeting held on Wednesday in Orlando, Fla.

"That is a significant statement," Leach said. "The PCI Council has never made this statement before - that through this effort you might be able to simplify your [PCI DSS] validation requirements." SC Magazine

Full Story :

[http://www.scmagazineus.com/pci-council-p2pe-simplifies-pci-dss-compliance/article/179439/?utm\\_source=feedburn](http://www.scmagazineus.com/pci-council-p2pe-simplifies-pci-dss-compliance/article/179439/?utm_source=feedburn)

## • Managing the cloud's security risks

Computerworld - Cloud computing is all the rage these days. CIOs seem to be diving into cloud-based solutions with reckless abandon despite the fact that a mistake in planning or execution can have career-limiting effects. So, let's take a moment to balance the benefits against the potential security pitfalls that lie in the clouds.

The really important question is, How safe is your business in the clouds? After all, cloud vendors all aim to put your stuff onto cloud servers, and in most cases, these systems sit outside of your data center and outside of your direct control.

While this may buy you some cost reductions, it carries significant risks. Let's consider the classic triad of information security: confidentiality, integrity and availability. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9187319/Managing\\_the\\_cloud\\_s\\_security\\_risks?source=rss\\_security](http://www.computerworld.com/s/article/9187319/Managing_the_cloud_s_security_risks?source=rss_security)

## • FBI investigating 'Here you have' worm

IDG News Service - The FBI has launched an investigation into the "Here you have" worm, which disrupted corporate e-mail systems in the U.S. two weeks ago.

Representatives from the FBI's Miami field office spoke with IDG News Service this week seeking information on the hacker behind the worm. A hacker using the name Iraq Resistance has exchanged a number of e-mails with IDG over the past two weeks discussing the incident.

"Here you have" was a big deal in North America, temporarily gumming up e-mail systems in large organizations such as Disney, Proctor & Gamble and NASA. On the day it was unleashed it accounted for between 6 percent and 14 percent of all spam on the Internet, according to Cisco Systems. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9187703/FBI\\_investigating\\_Here\\_you\\_have\\_worm?source=rss\\_security](http://www.computerworld.com/s/article/9187703/FBI_investigating_Here_you_have_worm?source=rss_security)

## • Report: Half of apps have security problems

This chart shows the source of application and the failure rate for security acceptance based on how critical the app is to the business.

(Credit: Veracode)

More than half of software used in enterprises has security problems, according to a new report to be released today from Veracode, an application security company. Cnet Security

Full Story :

[http://news.cnet.com/8301-27080\\_3-20017011-245.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-27080_3-20017011-245.html?part=rss&subj=news&tag=2547-1_3-0-20)

# New Vulnerabilities Tested in SecureScout

## • 18922 QuickTime heap buffer overflow in the handling of RLE encoded movie files (Remote File Checking)

A heap buffer overflow in the handling of RLE encoded movie files. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution. This issue is addressed by performing additional validation of RLE encoded movie files.

The issue has been fixed in version 7.6.6.

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

### References:

\* BUGTRAQ: 20100402 ZDI-10-040: Apple QuickTime RLE Bit Depth Remote Code Execution Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/510513/100/0/threaded>

\* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-10-040>

\* CONFIRM:

<http://support.apple.com/kb/HT4077>

\* APPLE: APPLE-SA-2010-03-29-1

<http://lists.apple.com/archives/security-announce/2010/Mar/msg00001.html>

\* APPLE: APPLE-SA-2010-03-30-1

<http://lists.apple.com/archives/security-announce/2010/Mar/msg00002.html>

\* OVAL: oval:org.mitre.oval:def:7062

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7062>

#### CVE Reference:

CVE-2010-0516 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18923 QuickTime heap buffer overflow in the handling of M-JPEG encoded movie files (Remote File Checking)

A heap buffer overflow in the handling of M-JPEG encoded movie files. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution. This issue is addressed by performing additional validation of M-JPEG encoded movie files.

The issue has been fixed in version 7.6.6.

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

#### References:

\* BUGTRAQ: 20100402 ZDI-10-037: Apple QuickTime MJPEG Sample Dimensions Remote Code Execution Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/510511/100/0/threaded>

\* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-10-037>

\* CONFIRM:

<http://support.apple.com/kb/HT4077>

\* APPLE: APPLE-SA-2010-03-29-1

<http://lists.apple.com/archives/security-announce/2010/Mar/msg00001.html>

\* APPLE: APPLE-SA-2010-03-30-1

<http://lists.apple.com/archives/security-announce/2010/Mar/msg00002.html>

\* OVAL: oval:org.mitre.oval:def:6673

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6673>

#### CVE Reference:

CVE-2010-0517 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18924 QuickTime memory corruption issue exists in the handling of Sorenson encoded movie files (Remote File Checking)

A memory corruption issue exists in the handling of Sorenson encoded movie files. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution. This issue is addressed by performing additional validation of Sorenson encoded movie files.

The issue has been fixed in version 7.6.6.

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

#### References:

\* CONFIRM:

<http://support.apple.com/kb/HT4077>

\* APPLE: APPLE-SA-2010-03-29-1

<http://lists.apple.com/archives/security-announce/2010/Mar/msg00001.html>

\* APPLE: APPLE-SA-2010-03-30-1

<http://lists.apple.com/archives/security-announce/2010/Mar/msg00002.html>

\* OVAL: oval:org.mitre.oval:def:7077

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7077>

#### CVE Reference:

CVE-2010-0518 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18925 QuickTime integer overflow exists in the handling of FlashPix encoded movie files (Remote File Checking)

An integer overflow exists in the handling of FlashPix encoded movie files. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution. This issue is addressed through improved bounds checking.

The issue has been fixed in version 7.6.6.

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

## References:

- \* BUGTRAQ: 20100402 ZDI-10-043: Apple QuickTime FlashPix NumberOfTiles Remote Code Execution Vulnerability  
<http://www.securityfocus.com/archive/1/archive/1/510519/100/0/threaded>
- \* MISC:  
<http://www.zerodayinitiative.com/advisories/ZDI-10-043>
- \* CONFIRM:  
<http://support.apple.com/kb/HT4077>
- \* APPLE: APPLE-SA-2010-03-29-1  
<http://lists.apple.com/archives/security-announce/2010/Mar/msg00001.html>
- \* APPLE: APPLE-SA-2010-03-30-1  
<http://lists.apple.com/archives/security-announce/2010/Mar/msg00002.html>
- \* OVAL: oval:org.mitre.oval:def:7498  
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7498>

## CVE Reference:

CVE-2010-0519 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 18936 IIS Repeated Parameter Request Denial of Service Vulnerability (MS10-065/2267960) (Remote File Checking)

A denial of service vulnerability exists in Internet Information Services (IIS) that could allow an attacker who successfully exploited this vulnerability to interrupt service, causing the server to become un-responsive. An attacker could exploit the vulnerability by sending specially crafted URL requests to active server pages on a Web site hosted by IIS.

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

## References:

- \* MS: MS10-065  
<http://www.microsoft.com/technet/security/Bulletin/MS10-065.mspx>
- \* BID: 43140  
<http://www.securityfocus.com/bid/43140>
- \* VUPEN: VUPEN/ADV-2010-2386  
<http://www.vupen.com/english/advisories/2010/2386>
- \* SECTRACK: 1024440  
<http://securitytracker.com/alerts/2010/Sep/1024440.html>

## CVE Reference:

CVE-2010-1899 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 18937 Request Header Buffer Overflow Vulnerability (MS10-065/2267960) (Remote File Checking)

A remote code execution vulnerability exists in Internet Information Services (IIS) that an attacker could exploit by sending specially crafted HTTP requests to IIS servers with FastCGI enabled.

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

## References:

- \* MS: MS10-065  
<http://www.microsoft.com/technet/security/Bulletin/MS10-065.mspx>
- \* BID: 43138  
<http://www.securityfocus.com/bid/43138>
- \* VUPEN: VUPEN/ADV-2010-2386  
<http://www.vupen.com/english/advisories/2010/2386>
- \* SECTRACK: 1024440  
<http://securitytracker.com/alerts/2010/Sep/1024440.html>

## CVE Reference:

CVE-2010-2730 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 18938 Directory Authentication Bypass Vulnerability (MS10-065/2267960) (Remote File Checking)

An elevation of privilege vulnerability exists in Internet Information Services (IIS). An attacker who successfully exploited this vulnerability could bypass the need to authenticate to access restricted resources.

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

## References:

\* MS: MS10-065  
<http://www.microsoft.com/technet/security/Bulletin/MS10-065.mspx>  
\* BID: 41314  
<http://www.securityfocus.com/bid/41314>  
\* VUPEN: VUPEN/ADV-2010-2386  
<http://www.vupen.com/english/advisories/2010/2386>  
\* SECTRACK: 1024440  
<http://securitytracker.com/alerts/2010/Sep/1024440.html>

**CVE Reference:**

CVE-2010-2731 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **18939 RPC Memory Corruption Vulnerability (MS10-066/982802) (Remote File Checking)**

An unauthenticated remote code execution vulnerability exists in the way that the Remote Procedure Call (RPC) client implementation allocates memory when parsing specially crafted RPC responses. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted RPC response to a client-initiated RPC request. An attacker who successfully exploited this vulnerability could execute arbitrary code and 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.

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

**References:**

\* MS: MS10-066  
<http://www.microsoft.com/technet/security/Bulletin/MS10-066.mspx>  
\* BID: 43119  
<http://www.securityfocus.com/bid/43119>  
\* VUPEN: VUPEN/ADV-2010-2387  
<http://www.vupen.com/english/advisories/2010/2387>

**CVE Reference:**

CVE-2010-2567 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **18940 CSRSS Local Elevation of Privilege Vulnerability (MS10-069/2121546) (Remote File Checking)**

An elevation of privilege vulnerability exists in the Windows CSRSS due to the way that the CSRSS assigns memory for specific user transactions. An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

**References:**

\* MS: MS10-069  
<http://www.microsoft.com/technet/security/Bulletin/MS10-069.mspx>  
\* BID: 43121  
<http://www.securityfocus.com/bid/43121>  
\* VUPEN: VUPEN/ADV-2010-2390  
<http://www.vupen.com/english/advisories/2010/2390>  
\* SECTRACK: 1024444  
<http://securitytracker.com/alerts/2010/Sep/1024444.html>

**CVE Reference:**

CVE-2010-1891 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **18941 LSASS Heap Overflow Vulnerability (MS10-068/983539) (Remote File Checking)**

An authenticated elevation of privilege vulnerability exists in Microsoft Windows due to the way that the Local Security Authority Subsystem Service (LSASS) improperly handles certain Lightweight Directory Access Protocol (LDAP) messages. The vulnerability exists in implementations of Active Directory, Active Directory Application Mode (ADAM), and Active Directory Lightweight Directory Service (AD LDS). An attacker must have previously authenticated with the LSASS server prior to exploiting this issue. An attacker who successfully exploited this vulnerability could execute arbitrary code and 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.

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

**References:**

\* MS: MS10-068

<http://www.microsoft.com/technet/security/Bulletin/MS10-068.msp>

\* BID: 43037

<http://www.securityfocus.com/bid/43037>

\* VUPEN: VUPEN/ADV-2010-2389

<http://www.vupen.com/english/advisories/2010/2389>

\* SECTRACK: 1024443

<http://securitytracker.com/alerts/2010/Sep/1024443.html>

#### **CVE Reference:**

CVE-2010-0820 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## **New Vulnerabilities found this Week**

### **• CVE-2010-3332 Microsoft CVSS 2.0 Score = 5.0**

Microsoft .NET Framework 1.0 SP3, 1.1 SP1, 2.0 SP2, 3.5, 3.5 SP1, 3.5.1, and 4.0, as used for ASP.NET in Microsoft Internet Information Services (IIS), provides detailed error codes during decryption attempts, which allows remote attackers to decrypt and modify encrypted View State (aka \_\_VIEWSTATE) form data, and possibly forge cookies or read application files, via a padding oracle attack.

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

#### **References:**

XF: <http://xforce.iss.net/xforce/xfdb/61898>

VUPEN: <http://www.vupen.com/english/advisories/2010/2429>

MISC: <http://www.troyhunt.com/2010/09/fear-uncertainty-and-and-padding-oracle.html>

MISC: <http://www.theinquirer.net/inquirer/news/1732956/security-researchers-destroy-microsoft-aspnet-security>

BID: <http://www.securityfocus.com/bid/43316>

CONFIRM: <http://www.microsoft.com/technet/security/advisory/2416728.msp>

MISC: <http://www.ekoparty.org/juliano-rizzo-2010.php>

MISC:

<http://www.dotnetnuke.com/Community/Blogs/tabid/825/EntryId/2799/Oracle-Padding-Vulnerability-in-ASP-NET.aspx>

CONFIRM: <http://weblogs.asp.net/scottgu/archive/2010/09/18/important-asp-net-security-vulnerability.aspx>

MISC: <http://twitter.com/thaidn/statuses/24832350146>

MISC: [http://threatpost.com/en\\_us/blogs/new-crypto-attack-affects-millions-aspnet-apps-091310](http://threatpost.com/en_us/blogs/new-crypto-attack-affects-millions-aspnet-apps-091310)

SECTRACK: <http://securitytracker.com/id?1024459>

SECUNIA: <http://secunia.com/advisories/41409>

MISC: <http://pentonizer.com/general-programming/aspnet-poet-vulnerability-what-else-can-i-do/>

MISC: <http://isc.sans.edu/diary.html?storyid=9568>

CONFIRM: <http://blogs.technet.com/b/srd/archive/2010/09/17/understanding-the-asp-net-vulnerability.aspx>

#### **CVE Reference: [CVE-2010-3332](#)**

### **• CVE-2010-3200 Microsoft CVSS 2.0 Score = 4.3**

MSO.dll in Microsoft Word 2003 SP3 11.8326.11.8324 allows remote attackers to cause a denial of service (NULL pointer dereference and multiple-instance application crash) via a crafted buffer in a Word document, as demonstrated by word\_crash\_11.8326.8324\_poc.doc.Per: <http://cwe.mitre.org/data/definitions/476.html> 'CWE-476: NULL Pointer Dereference'

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

**References:**

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/513679/100/0/threaded>

**CVE Reference:** [CVE-2010-3200](#)

**• CVE-2009-5002 IBM CVSS 2.0 Score = 6.4**

The Workplace (aka WP) component in IBM FileNet P8 Application Engine (P8AE) 4.0.2.x before 4.0.2.1-P8AE-FP001 does not record Get Content Failure Audit events, which might allow remote attackers to attempt content access without detection.

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

**References:**

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PJ34853>

CONFIRM: <http://download2.boulder.ibm.com/sar/CMA/IMA/00y3y/0/readme-4027-P8AE-FP007.htm>

**CVE Reference:** [CVE-2009-5002](#)

**• CVE-2010-3473 IBM CVSS 2.0 Score = 5.8**

Open redirect vulnerability in the Workplace (aka WP) component in IBM FileNet P8 Application Engine (P8AE) 3.5.1 before 3.5.1-021 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.

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

**References:**

VUPEN: <http://www.vupen.com/english/advisories/2010/2419>

BID: <http://www.securityfocus.com/bid/43272>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PJ37180>

SECUNIA: <http://secunia.com/advisories/41458>

CONFIRM: <http://download2.boulder.ibm.com/sar/CMA/IMA/00yrk/0/readme-ae351-021.htm>

**CVE Reference:** [CVE-2010-3473](#)

**• CVE-2010-3474 IBM CVSS 2.0 Score = 5.0**

IBM DB2 9.7 before FP3 does not perform the expected drops or invalidations of dependent functions upon a loss of privileges by the functions' owners, which allows remote authenticated users to bypass intended access restrictions via calls to these functions, a different vulnerability than CVE-2009-3471.

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

**References:**

XF: <http://xforce.iss.net/xforce/xfdb/61872>

VUPEN: <http://www.vupen.com/english/advisories/2010/2425>

BID: <http://www.securityfocus.com/bid/43291>

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg21446455>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg11C68015>

SECUNIA: <http://secunia.com/advisories/41444>

**CVE Reference:** [CVE-2010-3474](#)

**• CVE-2009-4999 IBM CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in the Workplace (aka WP) component in IBM FileNet P8 Application Engine (P8AE) 3.5.1 before 3.5.1-016 allows remote attackers to inject arbitrary web script or HTML via the Name field.

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

**References:**

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PJ34852>

CONFIRM: <http://download2.boulder.ibm.com/sar/CMA/IMA/00yrk/0/readme-ae351-021.htm>

**CVE Reference:** [CVE-2009-4999](#)

• **CVE-2009-5000 IBM CVSS 2.0 Score = 4.3**

Multiple cross-site scripting (XSS) vulnerabilities in the Workplace (aka WP) component in IBM FileNet P8 Application Engine (P8AE) 4.0.2.x before 4.0.2.3-P8AE-FP003 allow remote attackers to inject arbitrary web script or HTML via unspecified parameters to .jsp pages.

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

**References:**

CONFIRM: <http://download2.boulder.ibm.com/sar/CMA/IMA/00y3y/0/readme-4027-P8AE-FP007.htm>

**CVE Reference:** [CVE-2009-5000](#)

• **CVE-2010-3470 IBM CVSS 2.0 Score = 4.3**

Multiple cross-site scripting (XSS) vulnerabilities in the Workplace (aka WP) component in IBM FileNet P8 Application Engine (P8AE) 3.5.1 before 3.5.1-021 and 4.0.2.x before 4.0.2.7-P8AE-FP007 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.

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

**References:**

VUPEN: <http://www.vupen.com/english/advisories/2010/2419>

BID: <http://www.securityfocus.com/bid/43272>

BID: <http://www.securityfocus.com/bid/43271>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PJ37179>

SECUNIA: <http://secunia.com/advisories/41460>

SECUNIA: <http://secunia.com/advisories/41458>

CONFIRM: <http://download2.boulder.ibm.com/sar/CMA/IMA/00yrk/0/readme-ae351-021.htm>

CONFIRM: <http://download2.boulder.ibm.com/sar/CMA/IMA/00y3y/0/readme-4027-P8AE-FP007.htm>

**CVE Reference:** [CVE-2010-3470](#)

## 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)