

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 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.

This Week in Review

EU angry at bank for informing U.S. authorities. Standards are good but not enough. The new chief is the CPO. Hackers leave thir malware inactive on virtual machines.

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

❖ Data agency broke privacy laws

Gave personal data to U.S. authorities for use in anti-terror investigations
BRUSSELS, Belgium - A report by an EU panel released Thursday said the bank data transfer agency SWIFT broke European privacy laws by handing over personal data to U.S. authorities for use in anti-terror investigations.

The Belgian-based company, the Society for Worldwide Interbank Financial Telecommunication, "committed violations of data protection laws" by secretly

transferring data to the United States, without properly informing Belgian authorities, the EU's data protection panel said.

The panel's report calls on SWIFT, financial institutions and EU authorities to "take the necessary measures" to end the transfer, which it said contradicts Belgian and EU data protection rules. SWIFT is still transferring data under U.S. subpoenas.

MSNBC

Full Story :

<http://www.msnbc.msn.com/id/15916822/>

❖ Web Services Security Standards Aren't Enough

Enterprise professionals comforted by Web services security standards -- proposed or established -- may want to think again. Although useful for securing Web services messages, the specifications do little to safeguard against SOAP array overflow attacks and other ways of penetrating the back-end systems of an enterprise. With names such as WS-Security and SAML (Security Assertion Markup Language), it's understandable that practitioners might expect these standards to provide a framework for locking down their Web services applications.

For the most part, however, they don't.

"These standards do not deal with how you prevent attacks from happening," says Tony Baer, principal at onStrategies. "Standards are all about how you define the policy. Its all about handshaking."

WS-Security, among the most popular and mature of the standards, was developed by a coalition of vendors under the umbrella of OASIS, the prime standards body for Web services. It specifies the types of encryption and authentication that messages need -- for instance, SAML tokens, PKI, or Kerberos -- before they will be accepted and acted on. That ought to give the payment department at a large insurance company more confidence that the XML message requesting a US\$250,000 claim check is, in fact, from a trusted party.

But security experts hold little hope that WS-Security -- or any of its brethren, including WS-Trust or WS-SecurityPolicy -- will be enough to secure Web services, particularly if developers continue to write insecure code.

CIO news

Full Story :

<http://www.cio.in/news/viewArticle/ARTICLEID=2445>

❖ The What and Why of CPOs

Five years ago, privacy was a white-hot noun. Global 2,000 organizations were falling all over themselves trying to establish privacy organizations and policies. At that time, security guru Bill Malik, former head of Gartner's security practice, commented, "The chief privacy officer is a trend whose time has come."

Fast-forward to today. We are still waiting for the high-impact, change-my-stock-price and delight-my-customer CPO to show up and make his presence felt organizationally.

In 2006, many futurists believe we may be standing at the beginning of the largest and most life-changing technology expansion since the invention of fire. (Interestingly, it is Sarbanes-Oxley — initially labeled as an innovation-sucking bit of legislation that would do little more than provide full employment for bureaucrats — that may be viewed in the end as the great accelerator toward a truly digital society.) Future-focused organizations are getting their information management houses in order and tightening up internal processes in advance of the big takeoff. Among the things most in need of rethinking are privacy management and the chief privacy officer.

It's worthwhile, then, to consider questions regarding what CPOs do and why they're needed.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=273955&taxonomyId=17&intsrc=kc_feat

❖ Hackers Use New Tricks to Evade Detection

An increasing number of hackers build code that can detect when their virus is being run on a virtual machine. "This isn't a terribly new twist, but I have been seeing an increase over the last six weeks," said Roger Thompson, CTO of Exploit Prevention Labs. The trend is bound to continue as hackers tend to adopt proven strategies.

Hackers are incorporating virtual machine detection into their Trojans, worms and other malware in order to thwart antivirus vendors and virus Stop spam, spyware and viruses with Barracuda Networks' free evaluation unit. researchers, according to a note published this week by the SANS Institute Internet Storm Center.

Researchers often use virtual machines to detect hacker Latest News about hacker activities.

Virtual machines -- software that mimics a computer's hardware -- are useful for virus-testing, explained Roger Thompson, CTO of Exploit Prevention Labs. "You can run a virus to see what it does and then delete it when you are finished," he told TechNewsWorld.

An increasing number of hackers build code that can detect when their virus is being run on a virtual machine. "This isn't a terribly new twist, but I have been seeing an increase over the last six weeks," Thompson added.

LinuxInsider

Full Story :

<http://www.linuxinsider.com/story/security/54411.html>

New Vulnerabilities Tested in SecureScout

❖ 12148 SSL Server Outdated SSL protocol version Vulnerability

SSL is a network layer that allows privacy in communications. Servers supporting SSL should use the latest available version of the protocol.

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

References:

About the risk of using invalid certificates:

http://www.rsasecurity.com/products/keon/datasheets/KWS_DS_0702.pdf

Mozilla wiki:

http://wiki.mozilla.org/Necko:SSL_v2_Sites

CVE Reference:

❖ 13155 Solaris X Font Service Buffer Overflow

ISS X-Force has discovered a vulnerability in the Sun Microsystems implementation of the "X Window Font Service", or "XFS". The XFS service was designed as a component of the X Windows systems to establish a common mechanism to export font data to all computers on an X Windows network. A buffer overflow vulnerability exists within the XFS service (fs.auto).

Remote attackers can exploit the buffer overflow vulnerability to run arbitrary commands on a target system. Attackers must exploit this vulnerability in conjunction with another attack to gain "root" access, because the fs.auto service does not run with superuser privilege. The Solaris operating system is configured to run the fs.auto service by default. It is bound to a high TCP port, which is normally blocked on perimeter firewalls. Networks that are not filtering high TCP ports, and internal networks are potentially at risk.

This test case relied solely on the detection of the service to issue this warning and was unable to verify remotely whether you are vulnerable. Please verify the target has applied the appropriate patches.

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

References:

Original advisory:

<http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21541>

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-48879-1>

CVE Reference: [CVE-2002-1317](#)

❖ 13476 Oracle Database Server - JDBC component unspecified Vulnerability (Alert 68/aug-04/DB18)

CVE Reference: [CVE-2004-0637](#)
[CAN-2004-0638](#)

[CAN-2004-1338](#)
[CAN-2004-1339](#)
[CAN-2004-1362](#)
[CAN-2004-1363](#)
[CAN-2004-1364](#)
[CAN-2004-1366](#)
[CAN-2004-1367](#)
[CAN-2004-1368](#)
[CAN-2004-1369](#)
[CAN-2004-1370](#)

❖ **13477 Oracle Database Server - DDL component unspecified Vulnerability (Alert 68/aug-04/DB19)**

An unspecified vulnerability exists in Oracle Database Server DDL component.

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

References:

Original Advisory:

<http://www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf>

Other references:

iDEFENSE:

<http://www.iddefense.com/application/poi/display?id=135&type=vulnerabilities>

<http://www.iddefense.com/application/poi/display?id=136&type=vulnerabilities>

Red Database Security:

http://www.red-database-security.com/advisory/advisory_20040903_1.html

http://www.red-database-security.com/advisory/advisory_20040903_2.html

http://www.red-database-security.com/advisory/advisory_20040903_3.html

Application Security:

<http://www.appsecinc.com/resources/alerts/oracle/2004-0001/>

Integrigy:

<http://www.integrigy.com/alerts/OraAlert68OraAppsImpact.htm>

Pentest Limited:

<http://www.pentest.co.uk/documents/ptl-2004-04.html>

US-CERT VU#170830:

<http://www.kb.cert.org/vuls/id/170830>

US-CERT VU#435974:

<http://www.kb.cert.org/vuls/id/435974>

US-CERT VU#316206:

<http://www.kb.cert.org/vuls/id/316206>

BID:11099

<http://www.securityfocus.com/bid/11099>

BID:11100

<http://www.securityfocus.com/bid/11100>

BID:10871

<http://www.securityfocus.com/bid/10871>

<http://secunia.com/advisories/12409/>

<http://www.oracle.com/>

CVE Reference: [CVE-2004-0637](#)
[CAN-2004-0638](#)
[CAN-2004-1338](#)
[CAN-2004-1339](#)
[CAN-2004-1362](#)
[CAN-2004-1363](#)
[CAN-2004-1364](#)
[CAN-2004-1366](#)
[CAN-2004-1367](#)
[CAN-2004-1368](#)
[CAN-2004-1369](#)
[CAN-2004-1370](#)

❖ **13478 Oracle Database Server - Scheduler component unspecified Vulnerability (Alert 68/aug-04/DB20)**

An unspecified vulnerability exists in Oracle Database Server Scheduler component.

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

References:

Original Advisory:

<http://www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf>

Other references:

iDEFENSE:

<http://www.iddefense.com/application/poi/display?id=135&type=vulnerabilities>

<http://www.iddefense.com/application/poi/display?id=136&type=vulnerabilities>

Red Database Security:

http://www.red-database-security.com/advisory/advisory_20040903_1.html

http://www.red-database-security.com/advisory/advisory_20040903_2.html

http://www.red-database-security.com/advisory/advisory_20040903_3.html

Application Security:

<http://www.appsecinc.com/resources/alerts/oracle/2004-0001/>

Integrigy:

<http://www.integrigy.com/alerts/OraAlert68OraAppsImpact.htm>

Pentest Limited:

<http://www.pentest.co.uk/documents/ptl-2004-04.html>

US-CERT VU#170830:

<http://www.kb.cert.org/vuls/id/170830>

US-CERT VU#435974:

<http://www.kb.cert.org/vuls/id/435974>

US-CERT VU#316206:

<http://www.kb.cert.org/vuls/id/316206>

BID:11099

<http://www.securityfocus.com/bid/11099>

BID:11100

<http://www.securityfocus.com/bid/11100>

BID:10871

<http://www.securityfocus.com/bid/10871>

Secunia:

<http://secunia.com/advisories/12409/>

Product Homepage:

<http://www.oracle.com/>

CVE Reference: [CVE-2004-0637](#)
 [CAN-2004-0638](#)
 [CAN-2004-1338](#)
 [CAN-2004-1339](#)
 [CAN-2004-1362](#)
 [CAN-2004-1363](#)
 [CAN-2004-1364](#)
 [CAN-2004-1366](#)
 [CAN-2004-1367](#)
 [CAN-2004-1368](#)
 [CAN-2004-1369](#)
 [CAN-2004-1370](#)

❖ **13479 An unspecified vulnerability exists in Oracle Database Server Listener component.**

The vulnerability can be exploited to cause a DoS (Denial of Service), or conduct SQL injection attacks.

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

References:

Original Advisory:

<http://www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf>

Other references:

iDEFENSE:

<http://www.iddefense.com/application/poi/display?id=135&type=vulnerabilities>

<http://www.iddefense.com/application/poi/display?id=136&type=vulnerabilities>

Red Database Security:

http://www.red-database-security.com/advisory/advisory_20040903_1.html

http://www.red-database-security.com/advisory/advisory_20040903_2.html

http://www.red-database-security.com/advisory/advisory_20040903_3.html

Application Security:

<http://www.appsecinc.com/resources/alerts/oracle/2004-0001/>

Integrigy:

<http://www.integrigy.com/alerts/OraAlert68OraAppsImpact.htm>

Pentest Limited:

<http://www.pentest.co.uk/documents/ptl-2004-04.html>

US-CERT VU#170830:

<http://www.kb.cert.org/vuls/id/170830>

US-CERT VU#435974:

<http://www.kb.cert.org/vuls/id/435974>

US-CERT VU#316206:

<http://www.kb.cert.org/vuls/id/316206>

BID:11099

<http://www.securityfocus.com/bid/11099>

BID:11100

<http://www.securityfocus.com/bid/11100>

BID:10871

<http://www.securityfocus.com/bid/10871>

Secunia:

<http://secunia.com/advisories/12409/>

Product Homepage:

<http://www.oracle.com/>

CVE Reference: [CVE-2004-0637](#)
[CAN-2004-0638](#)
[CAN-2004-1338](#)
[CAN-2004-1339](#)
[CAN-2004-1362](#)
[CAN-2004-1363](#)
[CAN-2004-1364](#)
[CAN-2004-1366](#)
[CAN-2004-1367](#)
[CAN-2004-1368](#)
[CAN-2004-1369](#)
[CAN-2004-1370](#)

❖ **13480 Oracle Database Server - mod_plsql component unspecified Vulnerability (Alert 68/aug-04/DB22)**

An unspecified vulnerability exists in Oracle Database Server mod_plsql component.

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

References:

Original Advisory:

<http://www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf>

Other references:

iDEFENSE:

<http://www.iddefense.com/application/poi/display?id=135&type=vulnerabilities>

<http://www.iddefense.com/application/poi/display?id=136&type=vulnerabilities>

Red Database Security:

http://www.red-database-security.com/advisory/advisory_20040903_1.html

http://www.red-database-security.com/advisory/advisory_20040903_2.html

http://www.red-database-security.com/advisory/advisory_20040903_3.html

Application Security:

<http://www.appsecinc.com/resources/alerts/oracle/2004-0001/>

Integrigy:

<http://www.integrigy.com/alerts/OraAlert68OraAppsImpact.htm>

Pentest Limited:

<http://www.pentest.co.uk/documents/ptl-2004-04.html>

US-CERT VU#170830:

<http://www.kb.cert.org/vuls/id/170830>

US-CERT VU#435974:

<http://www.kb.cert.org/vuls/id/435974>

US-CERT VU#316206:

<http://www.kb.cert.org/vuls/id/316206>

BID:11099

<http://www.securityfocus.com/bid/11099>

BID:11100

<http://www.securityfocus.com/bid/11100>

BID:10871

<http://www.securityfocus.com/bid/10871>

Secunia:

<http://secunia.com/advisories/12409/>

Product Homepage:

<http://www.oracle.com/>

CVE Reference: [CVE-2004-0637](#)
[CAN-2004-0638](#)
[CAN-2004-1338](#)
[CAN-2004-1339](#)
[CAN-2004-1362](#)
[CAN-2004-1363](#)
[CAN-2004-1364](#)
[CAN-2004-1366](#)
[CAN-2004-1367](#)
[CAN-2004-1368](#)
[CAN-2004-1369](#)
[CAN-2004-1370](#)

❖ **13481 Oracle Database Server - Core SQL component unspecified Vulnerability (Alert 68/aug-04/DB23)**

An unspecified vulnerability exists in Oracle Database Server Core SQL component.

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

References:

Original Advisory:

<http://www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf>

Other references:

iDEFENSE:

<http://www.iddefense.com/application/poi/display?id=135&type=vulnerabilities>

<http://www.iddefense.com/application/poi/display?id=136&type=vulnerabilities>

Red Database Security:

http://www.red-database-security.com/advisory/advisory_20040903_1.html

http://www.red-database-security.com/advisory/advisory_20040903_2.html

http://www.red-database-security.com/advisory/advisory_20040903_3.html

Application Security:

<http://www.appsecinc.com/resources/alerts/oracle/2004-0001/>

Integrigy:

<http://www.integrigy.com/alerts/OraAlert68OraAppsImpact.htm>

Pentest Limited:

<http://www.pentest.co.uk/documents/ptl-2004-04.html>

US-CERT VU#170830:

<http://www.kb.cert.org/vuls/id/170830>

US-CERT VU#435974:

<http://www.kb.cert.org/vuls/id/435974>

US-CERT VU#316206:

<http://www.kb.cert.org/vuls/id/316206>

BID:11099

<http://www.securityfocus.com/bid/11099>

BID:11100

<http://www.securityfocus.com/bid/11100>

BID:10871

<http://www.securityfocus.com/bid/10871>

Secunia:

<http://secunia.com/advisories/12409/>

Product Homepage:

<http://www.oracle.com/>

CVE Reference: [CVE-2004-0637](#)
[CAN-2004-0638](#)
[CAN-2004-1338](#)
[CAN-2004-1339](#)
[CAN-2004-1362](#)
[CAN-2004-1363](#)
[CAN-2004-1364](#)
[CAN-2004-1366](#)
[CAN-2004-1367](#)
[CAN-2004-1368](#)
[CAN-2004-1369](#)
[CAN-2004-1370](#)

❖ **13482 Oracle Database Server - Ultrasearch component unspecified Vulnerability (Alert 68/aug-04/DB24)**

An unspecified vulnerability exists in Oracle Database Server Ultrasearch component.

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

References:

Original Advisory:

<http://www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf>

Other references:

iDEFENSE:

<http://www.iddefense.com/application/poi/display?id=135&type=vulnerabilities>

<http://www.iddefense.com/application/poi/display?id=136&type=vulnerabilities>

Red Database Security:

http://www.red-database-security.com/advisory/advisory_20040903_1.html

http://www.red-database-security.com/advisory/advisory_20040903_2.html

http://www.red-database-security.com/advisory/advisory_20040903_3.html

Application Security:

<http://www.appsecinc.com/resources/alerts/oracle/2004-0001/>

Integrigy:

<http://www.integrigy.com/alerts/OraAlert68OraAppsImpact.htm>

Pentest Limited:

<http://www.pentest.co.uk/documents/ptl-2004-04.html>

US-CERT VU#170830:

<http://www.kb.cert.org/vuls/id/170830>

US-CERT VU#435974:

<http://www.kb.cert.org/vuls/id/435974>

US-CERT VU#316206:

<http://www.kb.cert.org/vuls/id/316206>

BID:11099

<http://www.securityfocus.com/bid/11099>

BID:11100

<http://www.securityfocus.com/bid/11100>

BID:10871

<http://www.securityfocus.com/bid/10871>

Secunia:

<http://secunia.com/advisories/12409/>

Product Homepage:

<http://www.oracle.com/>

CVE Reference: [CVE-2004-0637](#)
[CAN-2004-0638](#)
[CAN-2004-1338](#)
[CAN-2004-1339](#)
[CAN-2004-1362](#)
[CAN-2004-1363](#)
[CAN-2004-1364](#)
[CAN-2004-1366](#)
[CAN-2004-1367](#)
[CAN-2004-1368](#)
[CAN-2004-1369](#)
[CAN-2004-1370](#)

❖ **14744 Sun Kodak Color Management System (KCMS) library service daemon (kcms_server) arbitrary files reading Vulnerability**

It has been reported that a problem exists in the Kodak Color Management System (KCMS) due to the insecure handling of input. It may be possible for a remote user to gain access to arbitrary files on a vulnerable host. This could allow remote information gathering, leakage of sensitive information, and potentially privilege elevation.

This test case relied solely on the detection of the service to issue this warning and was unable to verify remotely whether you are vulnerable. Please verify the target has applied the appropriate patches.

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

References:

Original advisory:

SUNALERT:50104

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-50104-1>

Other references:

* BUGTRAQ:20030122 Entercept Ricochet Advisory: Sun Solaris KCMS Library Service Daemon Arbitrary File Retrieval Vulner

* URL:<http://marc.theaimsgroup.com/?l=bugtraq&m=104326556329850&w=2>

* MISC: <http://www.entercept.com/news/uspr/01-22-03.asp>

* CERT-VN:VU#850785

* URL:<http://www.kb.cert.org/vuls/id/850785>

* BID:6665

* URL:<http://www.securityfocus.com/bid/6665>

* XF:solaris-kcms-directory-traversal(11129)

* URL:<http://xforce.iss.net/xforce/xfdb/11129>

* OVAL:oval:org.mitre.oval:def:120

* URL:<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:120>

* OVAL:oval:org.mitre.oval:def:195

* URL:<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:195>

* OVAL:oval:org.mitre.oval:def:2592

* URL:<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2592>

CVE Reference: [CVE-2003-0027](#)

New Vulnerabilities found this Week

Apple Mac OS X UDIF Memory Corruption Vulnerability

“Gain escalated privileges”

LMH has reported a vulnerability in Mac OS X, which potentially can be exploited by malicious, local users to gain escalated privileges or by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an error in com.apple.AppleDiskImageController when handling corrupted DMG image structures. This can be exploited to cause a memory corruption and may allow execution of arbitrary code in kernel-mode.

The vulnerability is reported in a fully patched Mac OS X (2006-11-20). Other versions may also be affected.

References:

<http://projects.info-pull.com/mokb/MOKB-20-11-2006.html>

Novell Client NWSPool.DLL Unspecified Buffer Overflow Vulnerability

“Buffer overflow”

A vulnerability with an unknown impact has been reported in Novell Client.

The vulnerability is caused due to a possible buffer overflow in NWSPool.DLL. No more information is currently available.

References:

<http://support.novell.com/cgi-bin/search/searchtid.cgi?/2974765.htm>

XML-RPC for PHP PHP Code Execution Vulnerability

“Inject arbitrary PHP code”

James Bercegay has reported a vulnerability in XML-RPC for PHP, which can be exploited by malicious people to compromise a vulnerable system.

Input passed in an XML document is not properly sanitized before being used in an "eval()" call. This can be exploited to inject arbitrary PHP code via a specially crafted XML document.

The vulnerability has been reported in version 1.1 and prior.

References:

http://sourceforge.net/project/showfiles.php?group_id=34455

ProFTPD "CommandBufferSize" Denial of Service Vulnerability

“Denial of Service”

A vulnerability has been reported in ProFTPD, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error within the "cmd_loop()" function in main.c when the "CommandBufferSize" option is enabled.

References:

http://proftp.cvs.sourceforge.net/proftp/proftpd/src/main.c?view=diff&r1=text&tr1=1.292&r2=text&tr2=1.294&diff_format=h

NetGear WG111v2 Wireless Driver Beacon Request Buffer Overflow

“Stack-based buffer overflow; execution of arbitrary code”

A vulnerability has been reported in NetGear WG111v2 wireless driver, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the WG111v2.SYS driver when handling beacon requests. This can be exploited to cause a stack-based buffer overflow via a malicious beacon request containing more than 1100 bytes of information elements.

Successful exploitation allows execution of arbitrary code.

The vulnerability is reported in version 5.1213.6.316 of the WG111v2.SYS driver. Other versions may also be affected.

References:

<http://projects.info-pull.com/mokb/MOKB-16-11-2006.html>

<http://www.kb.cert.org/vuls/id/445753>

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