

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

[ASN.1 Vulnerability Scanner](#) - The S4 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.

Download Here:

<http://www.netvigilance.com/productdownloads?productname=asn.1vulnerabilityscanner>

This Week in Review

Money mule scam BIG. New european law on all electronic. New TLS and SSL flaw. US addresses cybersecurity standards.

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

• FBI: Money mule scams top \$100 million

Cybercriminals have attempted to steal \$100 million from small- and medium-sized businesses in so-called money mule scams, according to an intelligence note issued Wednesday by the bureau's Internet Crime Complaint Center (IC3).

Every week the FBI receives new victim complaints and opens new cases about these crimes, which often involve sophisticated banking trojans being placed on victim PCs. This then enables the perpetrators to siphon corporate online banking credentials and then transfer or wire money out of the account, IC3 said in its intelligence note. So far, cybercriminals have successfully stolen \$40 million in crimes of this nature, Brian Krebs at the Washington Post recently reported. SC Magazine

Full Story :

<http://www.scmagazineus.com/FBI-Money-mule-scams-top-100-million/article/157066/>

• Europe getting 'Internet freedom' law

Europe is set to get a major overhaul of its telecommunications regulation, after the European Parliament and Council of Telecoms Ministers reached a compromise on the rights of Internet users.

The Telecoms Reform Package is a raft of new laws that tackle issues ranging from data-breach notification to faster number porting. Following an agreement reached on Wednesday night, the package will now become part of national legislation in every EU country, with a deadline of May 2011. Cnet Security

Full Story :

http://news.cnet.com/8301-1035_3-10391474-94.html?part=rss&subj=news&tag=2547-1_3-0-20

• Zero-day flaw found in Web encryption

A zero-day flaw in the TLS and SSL protocols, which are commonly used to encrypt Web pages, has been made public.

Security researchers Marsh Ray and Steve Dispensa unveiled the TLS (Transport Layer Security) flaw on Wednesday, following the disclosure of separate, but similar, security findings. TLS and its predecessor, SSL (Secure Sockets Layer), are typically used by online retailers and banks to provide security for Web transactions.

Ray, who works with Dispensa at two-factor authentication company PhoneFactor, explained in a blog post this week that he had initially discovered the flaw in August and demonstrated a working exploit to Dispensa at the beginning of September. Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-10391485-83.html?part=rss&subj=news&tag=2547-1_3-0-20

• House panel OKs law addressing cyberstandards

A draft bill approved Wednesday by a House subcommittee would require the National Institute of Standards and Technology (NIST) to facilitate U.S. involvement in the creation of international cybersecurity standards.

The proposed Cybersecurity Coordination and Awareness Act, approved Wednesday by the House Subcommittee on Technology and Innovation, would also require NIST to develop and implement a cybersecurity awareness and education program and engage in research and development to improve identity management systems. Also, it would amend the Cybersecurity Research and Development Act to update technical terms. SC Magazine

Full Story :

<http://www.scmagazineus.com/House-panel-OKs-law-addressing-cyberstandards/article/157153/>

New Vulnerabilities Tested in SecureScout

• 13722 Oracle Database Server - Core RDBMS component unspecified Vulnerability (oct-2009/CVE-2009-1992)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Core RDBMS" component.

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html>

* CERT: TA09-294A

<http://www.us-cert.gov/cas/techalerts/TA09-294A.html>

* BID: 36742

<http://www.securityfocus.com/bid/36742>

* SECTRAK: 1023057

<http://www.securitytracker.com/id?1023057>

* SECUNIA: 37027

<http://secunia.com/advisories/37027>

CVE Reference:

CVE-2009-1992 (cve.mitre.org, nvd.nist.gov)

• 13723 Oracle Database Server - Network Authentication component unspecified Vulnerability (oct-2009/CVE-2009-1979)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Network Authentication" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html>
- * CERT: TA09-294A
<http://www.us-cert.gov/cas/techalerts/TA09-294A.html>
- * BID: 36747
<http://www.securityfocus.com/bid/36747>
- * OSVDB: 59110
<http://osvdb.org/59110>
- * SECTrack: 1023057
<http://www.securitytracker.com/id?1023057>
- * SECUNIA: 37027
<http://secunia.com/advisories/37027>

CVE Reference:

CVE-2009-1979 (cve.mitre.org, nvd.nist.gov)

• 13724 Oracle Database Server - Network Authentication component unspecified Vulnerability (oct-2009/CVE-2009-1985)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Network Authentication" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html>
- * CERT: TA09-294A
<http://www.us-cert.gov/cas/techalerts/TA09-294A.html>
- * BID: 36745
<http://www.securityfocus.com/bid/36745>
- * OSVDB: 59111
<http://osvdb.org/59111>
- * SECTrack: 1023057
<http://www.securitytracker.com/id?1023057>
- * SECUNIA: 37027
<http://secunia.com/advisories/37027>

CVE Reference:

CVE-2009-1985 (cve.mitre.org, nvd.nist.gov)

• 13725 Oracle Database Server - Data Mining component unspecified Vulnerability (oct-2009/CVE-2009-1007)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Data Mining" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html>
- * CERT: TA09-294A
<http://www.us-cert.gov/cas/techalerts/TA09-294A.html>
- * BID: 36750
<http://www.securityfocus.com/bid/36750>
- * SECTrack: 1023057
<http://www.securitytracker.com/id?1023057>
- * SECUNIA: 37027
<http://secunia.com/advisories/37027>

CVE Reference:

CVE-2009-1007 (cve.mitre.org, nvd.nist.gov)

• 13726 Oracle Database Server - Oracle Spatial component unspecified Vulnerability (oct-2009/CVE-2009-1994)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Oracle Spatial" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html>
- * CERT: TA09-294A
<http://www.us-cert.gov/cas/techalerts/TA09-294A.html>
- * BID: 36744
<http://www.securityfocus.com/bid/36744>
- * SECTrack: 1023057
<http://www.securitytracker.com/id?1023057>
- * SECUNIA: 37027
<http://secunia.com/advisories/37027>

CVE Reference:

CVE-2009-1994 (cve.mitre.org, nvd.nist.gov)

• 13727 Oracle Database Server - PL/SQL component unspecified Vulnerability (oct-2009/CVE-2009-2001)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "PL/SQL" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html>
- * CERT: TA09-294A
<http://www.us-cert.gov/cas/techalerts/TA09-294A.html>
- * BID: 36743
<http://www.securityfocus.com/bid/36743>
- * SECTrack: 1023057
<http://www.securitytracker.com/id?1023057>
- * SECUNIA: 37027
<http://secunia.com/advisories/37027>

CVE Reference:

CVE-2009-2001 (cve.mitre.org, nvd.nist.gov)

• 13729 Oracle Database Server - Workspace Manager component unspecified Vulnerability (oct-2009/CVE-2009-1018)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Workspace Manager" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html>
- * CERT: TA09-294A
<http://www.us-cert.gov/cas/techalerts/TA09-294A.html>
- * BID: 36765
<http://www.securityfocus.com/bid/36765>
- * OSVDB: 59112
<http://osvdb.org/59112>
- * SECTrack: 1023057
<http://www.securitytracker.com/id?1023057>
- * SECUNIA: 37027
<http://secunia.com/advisories/37027>

CVE Reference:

CVE-2009-1018 (cve.mitre.org, nvd.nist.gov)

• 13730 Oracle Database Server - Workspace Manager component unspecified Vulnerability (oct-2009/CVE-2009-1964)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Workspace Manager" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html>
- * CERT: TA09-294A
<http://www.us-cert.gov/cas/techalerts/TA09-294A.html>
- * BID: 36755
<http://www.securityfocus.com/bid/36755>
- * OSVDB: 59115
<http://osvdb.org/59115>
- * SECTrack: 1023057
<http://www.securitytracker.com/id?1023057>
- * SECUNIA: 37027
<http://secunia.com/advisories/37027>

CVE Reference:

CVE-2009-1964 (cve.mitre.org, nvd.nist.gov)

• 13731 Oracle Database Server - Net Foundation Layer component unspecified Vulnerability (oct-2009/CVE-2009-1965)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Net Foundation Layer" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html>
- * CERT: TA09-294A
<http://www.us-cert.gov/cas/techalerts/TA09-294A.html>
- * BID: 36760
<http://www.securityfocus.com/bid/36760>
- * SECTrack: 1023057
<http://www.securitytracker.com/id?1023057>
- * SECUNIA: 37027
<http://secunia.com/advisories/37027>

CVE Reference:

CVE-2009-1965 (cve.mitre.org, nvd.nist.gov)

• 13732 Oracle Database Server - Authentication component unspecified Vulnerability (oct-2009/CVE-2009-1997)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Authentication" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html>
- * CERT: TA09-294A
<http://www.us-cert.gov/cas/techalerts/TA09-294A.html>
- * BID: 36751
<http://www.securityfocus.com/bid/36751>
- * SECTrack: 1023057
<http://www.securitytracker.com/id?1023057>
- * SECUNIA: 37027
<http://secunia.com/advisories/37027>

CVE Reference:

CVE-2009-1997 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2009-3031 Symantec CVSS 2.0 Score = 9.3**

Stack-based buffer overflow in the BrowseAndSaveFile method in the Altiris eXpress NS ConsoleUtilities ActiveX control 6.0.0.1846 in AeXNSConsoleUtilities.dll in Symantec Altiris Notification Server (NS) 6.0 before R12, Deployment Server 6.8 and 6.9 in Symantec Altiris Deployment Solution 6.9 SP3, and Symantec Management Platform (SMP) 7.0 before SP3 allows remote attackers to execute arbitrary code via a long string in the second argument.

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

References:

CONFIRM:

http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory

CONFIRM: <https://kb.altiris.com/article.asp?article=49568&p=1>

CONFIRM: <https://kb.altiris.com/article.asp?article=49389&p=1>

VUPEN: <http://www.vupen.com/english/advisories/2009/3117>

BID: <http://www.securityfocus.com/bid/36698>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/507625/100/0/threaded>

MISC: <http://sotiriu.de/adv/NSOADV-2009-001.txt>

CVE Reference: [CVE-2009-3031](#)

• **CVE-2009-3854 IBM CVSS 2.0 Score = 10.0**

Buffer overflow in the traditional client scheduler in the client in IBM Tivoli Storage Manager (TSM) 5.3 before 5.3.6.7 and 5.4 before 5.4.2 allows remote attackers to execute arbitrary code via unspecified vectors.

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

References:

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21405562>

VUPEN: <http://www.vupen.com/english/advisories/2009/3132>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1IC61058>

CVE Reference: [CVE-2009-3854](#)

• **CVE-2009-0306 IBM CVSS 2.0 Score = 9.3**

Buffer overflow in the IBM Lotus Notes Intellisync ActiveX control in Inresobject.dll in BlackBerry Desktop Manager in Research In Motion (RIM) BlackBerry Desktop Software before 5.0.1 allows remote attackers to execute arbitrary code via a crafted web page. NOTE: some of these details are obtained from third party information.

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

References:

CONFIRM: <http://www.blackberry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB19701>

VUPEN: <http://www.vupen.com/english/advisories/2009/3133>

BID: <http://www.securityfocus.com/bid/36903>

CVE Reference: [CVE-2009-0306](#)

• **CVE-2009-3853 IBM CVSS 2.0 Score = 9.3**

Buffer overflow in the client acceptor daemon (CAD) scheduler in the client in IBM Tivoli Storage Manager (TSM) 5.3 before 5.3.6.7, 5.4 before 5.4.3, 5.5 before 5.5.2.2, and 6.1 before 6.1.0.2, and TSM Express 5.3.3.0 through 5.3.6.6, allows remote attackers to execute arbitrary code via unspecified vectors.

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

References:

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21405562>

VUPEN: <http://www.vupen.com/english/advisories/2009/3132>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1IC61036>

CVE Reference: [CVE-2009-3853](#)

• **CVE-2009-3855 IBM CVSS 2.0 Score = 9.3**

Multiple unspecified vulnerabilities in the (1) UNIX and (2) Linux backup-archive clients, and the (3) OS/400 API client, in IBM Tivoli Storage Manager (TSM) 5.3 before 5.3.6.6, 5.4 before 5.4.2, and 5.5 before 5.5.1, when the MAILPROG option is enabled, allow attackers to read, modify, or delete arbitrary files via unknown vectors.

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

References:

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21405562>

VUPEN: <http://www.vupen.com/english/advisories/2009/3132>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1IC54489>

CVE Reference: [CVE-2009-3855](#)

• **CVE-2009-3852 IBM CVSS 2.0 Score = 7.5**

Unspecified vulnerability in the XML component in IBM Runtimes for Java Technology 5.0.0 before SR10 has unknown impact and attack vectors, related to the "updated version of XML4J 4.4.17."

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/54069>

VUPEN: <http://www.vupen.com/english/advisories/2009/3106>

BID: <http://www.securityfocus.com/bid/36894>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1IZ63920>

SECUNIA: <http://secunia.com/advisories/37210>

CVE Reference: [CVE-2009-3852](#)

• **CVE-2009-3464 Adobe CVSS 2.0 Score = 10.0**

Adobe Shockwave Player before 11.5.2.602 allows remote attackers to execute arbitrary code via crafted Shockwave content on a web site, related to an "invalid pointer vulnerability," a different issue than CVE-2009-3465. NOTE: some of these details are obtained from third party information.

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

References:

BID: <http://www.securityfocus.com/bid/36905>

CONFIRM: <http://www.adobe.com/support/security/bulletins/apsb09-16.html>

XF: <http://xforce.iss.net/xforce/xfdb/54119>

VUPEN: <http://www.vupen.com/english/advisories/2009/3134>

SECTRAK: <http://securitytracker.com/id?1023123>

CVE Reference: [CVE-2009-3464](#)

• **CVE-2009-3465 Adobe CVSS 2.0 Score = 10.0**

Adobe Shockwave Player before 11.5.2.602 allows remote attackers to execute arbitrary code via crafted Shockwave content on a web site, related to an "invalid pointer vulnerability," a different issue than CVE-2009-3464. NOTE: some of these details are obtained from third party information.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/54120>

VUPEN: <http://www.vupen.com/english/advisories/2009/3134>

BID: <http://www.securityfocus.com/bid/36905>

CONFIRM: <http://www.adobe.com/support/security/bulletins/apsb09-16.html>

SECTRAK: <http://securitytracker.com/id?1023123>

CVE Reference: [CVE-2009-3465](#)

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