

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

Sharepoint XSS vulnerable. Higher data breach costs in US. Social Network site will focus on security after breach. Techie convicted for hijacking city network.

TechTip

To make your scan finish faster on Windows Workstation OS, (Windows XP, Vista and 7), increase background processing priority by changing the following setting: System Properties - Advanced Tab - Performance - Settings - Advanced Tab - Processor Scheduling - Background Services
No reboot required

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

• New SharePoint bug opens corporations to data loss risk

Microsoft warned Thursday of a cross-site scripting (XSS) vulnerability in its business collaborative platform SharePoint that could allow hackers to elevate privileges and steal sensitive data.

Users running Windows SharePoint Services 3.0 or Microsoft Office SharePoint Server 2007 are affected.

The flaw was disclosed to Microsoft earlier this month by Swiss security firm High-Tech Bridge. On Wednesday, the company, whose policy is to go public with bug details two weeks after notifying the vendor, issued an advisory, which included a link to a proof-of-concept code that exploits the vulnerability. SC Magazine

Full Story :

http://www.scmagazineus.com/new-sharepoint-bug-opens-corporations-to-data-loss-risk/article/169159/?utm_source=

• U.S. organizations face the highest data breach costs

Organizations in the United States incurred the highest costs associated with data breaches last year compared to businesses located in other countries, according to a report released Wednesday by the Ponemon Institute. The report, sponsored by encryption firm PGP, assessed the costs of activities resulting from more than 100 data breach incidents affecting organizations in the United States, U.K., Australia, France and Germany. Breach costs were much higher for organizations located in countries with notification laws, such as the United States, according to the study.

In the United States, where 46 states have enacted laws mandating customers be alerted if their personal information has been exposed, breach costs were 43 percent higher than the global average. SC Magazine

Full Story :

http://www.scmagazineus.com/us-organizations-face-the-highest-data-breach-costs/article/169160/?utm_source=fee

• Blippy to hire CSO, conduct audits after credit card breach

Blippy, a Silicon Valley start-up that enables users to share details in real time about purchases they make, plans to invest millions in information security following revelations that it exposed the credit card numbers of a small number of people through Google's search index.

Ashvin Kumar, co-founder and CEO of Blippy, said in a blog post early Monday that as a result of the breach the company plans to hire a CSO, conduct regular third-party security audits, and install technology that strips out sensitive information from Blippy posts. In addition, the firm plans to create a central portal for users to obtain information about security and privacy. SC Magazine

Full Story :

http://www.scmagazineus.com/blippy-to-hire-cso-conduct-audits-after-credit-card-breach/article/168728/?utm_source=

• Ex-SF tech convicted of hijacking city network

A former San Francisco network administrator was convicted Tuesday of hijacking the city's computer network and refusing to provide passwords to his superiors.

Terry Childs, who had worked at San Francisco's Department of Telecommunication Information Services for 10 years, was found guilty of a felony charge of denying computer access and faces a maximum state prison sentence of five years, according to a San Francisco Chronicle report. Judge Teri Jackson is expected to factor in time already served for Childs, who has been in custody since July 2008.

Childs, 45, tampered with the city's Fiber Wide Area Network, which maintains about 60 percent of the city's law enforcement, payroll, and jail-booking records, after reportedly becoming agitated over pending layoffs. He was also accused of electronically spying on his supervisors and their attempt to fire him, but those charges were dismissed last August. Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-20003611-83.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• 13751 Oracle Database Server - Oracle Internet Directory component unspecified Vulnerability (apr-2010/CVE-2010-0853)

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

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2010.html>

* CERT: TA10-103B

<http://www.us-cert.gov/cas/techalerts/TA10-103B.html>

* SECUNIA: 39438

<http://secunia.com/advisories/39438>

* SECUNIA: 39439

<http://secunia.com/advisories/39439>

* BID: 39418
<http://www.securityfocus.com/bid/39418>
* SECTRACK: 1023870
<http://securitytracker.com/alerts/2010/Apr/1023870.html>
* VUPEN: VUPEN/ADV-2010-0878
<http://www.vupen.com/english/advisories/2010/0878>

CVE Reference:

CVE-2010-0853 (cve.mitre.org, nvd.nist.gov)

• **13752 Oracle Database Server - Core RDBMS component unspecified Vulnerability (apr-2010/CVE-2010-0860)**

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:

* BID: 39439
<http://www.securityfocus.com/bid/39439>
* SECTRACK: 1023858
<http://securitytracker.com/alerts/2010/Apr/1023858.html>
* VUPEN: VUPEN/ADV-2010-0878
<http://www.vupen.com/english/advisories/2010/0878>
* CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2010.html>
* CERT: TA10-103B
<http://www.us-cert.gov/cas/techalerts/TA10-103B.html>
* SECUNIA: 39438
<http://secunia.com/advisories/39438>

CVE Reference:

CVE-2010-0860 (cve.mitre.org, nvd.nist.gov)

• **13753 Oracle Database Server - Core RDBMS component unspecified Vulnerability (apr-2010/CVE-2010-0866)**

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

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

References:

* BID: 39424
<http://www.securityfocus.com/bid/39424>
* SECTRACK: 1023858
<http://securitytracker.com/alerts/2010/Apr/1023858.html>
* VUPEN: VUPEN/ADV-2010-0878
<http://www.vupen.com/english/advisories/2010/0878>
* CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2010.html>
* CERT: TA10-103B
<http://www.us-cert.gov/cas/techalerts/TA10-103B.html>

CVE Reference:

CVE-2010-0866 (cve.mitre.org, nvd.nist.gov)

• **13754 Oracle Database Server - Core RDBMS component unspecified Vulnerability (apr-2010/CVE-2010-0852)**

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

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

References:

* BID: 39421
<http://www.securityfocus.com/bid/39421>
* SECTRACK: 1023858
<http://securitytracker.com/alerts/2010/Apr/1023858.html>
* VUPEN: VUPEN/ADV-2010-0878

<http://www.vupen.com/english/advisories/2010/0878>

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2010.html>

* CERT: TA10-103B

<http://www.us-cert.gov/cas/techalerts/TA10-103B.html>

* SECUNIA: 39438

<http://secunia.com/advisories/39438>

CVE Reference:

CVE-2010-0852 (cve.mitre.org, nvd.nist.gov)

• 18781 MPEG Layer-3 Audio Decoder Stack Overflow Vulnerability (MS10-026/977816) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft MPEG Layer-3 codecs handle AVI media files. This vulnerability could allow remote code execution if a user opened a specially crafted AVI file containing an MPEG Layer-3 audio stream. 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.

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

References:

* MS: MS10-026

<http://www.microsoft.com/technet/security/Bulletin/MS10-026.mspx>

* CERT: TA10-103A

<http://www.us-cert.gov/cas/techalerts/TA10-103A.html>

* VUPEN: VUPEN/ADV-2010-0869

<http://www.vupen.com/english/advisories/2010/0869>

* BID: 39303

<http://www.securityfocus.com/bid/39303>

* SECTRACK: 1023848

<http://securitytracker.com/alerts/2010/Apr/1023848.html>

CVE Reference:

CVE-2010-0480 (cve.mitre.org, nvd.nist.gov)

• 18782 VBScript Help Keypress Vulnerability (MS10-022/981169) (Remote File Checking)

A remote code execution vulnerability exists in the way that VBScript interacts with Windows Help files when using Internet Explorer. If a malicious Web site displayed a specially crafted dialog box and a user pressed the F1 key, the Windows Help System would be started with a Windows Help File provided by the attacker. 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. On systems running Windows Server 2003, Internet Explorer Enhanced Security Configuration is enabled by default, which helps to mitigate against this issue.

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

References:

* MISC:

<http://isec.pl/vulnerabilities/isec-0027-msgbox-helpfile-ie.txt>

* MISC:

<http://isec.pl/vulnerabilities10.html>

* MISC:

http://www.computerworld.com/s/article/9163298/New_zero_day_involves_IE_puts_Windows_XP_users_at_risk

* MISC:

http://www.theregister.co.uk/2010/03/01/ie_code_execution_bug/

* CONFIRM:

<http://blogs.technet.com/msrc/archive/2010/02/28/investigating-a-new-win32hlp-and-internet-explorer-issue.aspx>

* CONFIRM:

<http://blogs.technet.com/msrc/archive/2010/03/01/security-advisory-981169-released.aspx>

* CONFIRM:

<http://blogs.technet.com/srd/archive/2010/03/01/help-keypress-vulnerability-in-vbscript-enabling-remote-code-execution.aspx>

* CONFIRM:

<http://www.microsoft.com/technet/security/advisory/981169.mspx>

* MS: MS10-022

<http://www.microsoft.com/technet/security/Bulletin/MS10-022.msp>

* CERT: TA10-103A

<http://www.us-cert.gov/cas/techalerts/TA10-103A.html>

* CERT-VN: VU#612021

<http://www.kb.cert.org/vuls/id/612021>

* BID: 38463

<http://www.securityfocus.com/bid/38463>

* OSVDB: 62632

<http://www.osvdb.org/62632>

* SECTRACK: 1023668

<http://securitytracker.com/id?1023668>

* SECUNIA: 38727

<http://secunia.com/advisories/38727>

* VUPEN: ADV-2010-0485

<http://www.vupen.com/english/advisories/2010/0485>

* XF: ms-win-msgbox-code-execution(56558)

<http://xforce.iss.net/xforce/xfdb/56558>

CVE Reference:

CVE-2010-0483 (cve.mitre.org, nvd.nist.gov)

• 18783 Microsoft Office Publisher File Conversion TextBox Processing Buffer Overflow Vulnerability (MS10-023/981160) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Publisher opens Publisher files. An attacker could exploit the vulnerability by creating a specially crafted Publisher file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site, and then convincing the user to open the specially crafted Publisher 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 user rights.

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

References:

* MS: MS10-023

<http://www.microsoft.com/technet/security/Bulletin/MS10-023.msp>

* CERT: TA10-103A

<http://www.us-cert.gov/cas/techalerts/TA10-103A.html>

* VUPEN: VUPEN/ADV-2010-0866

<http://www.vupen.com/english/advisories/2010/0866>

* BID: 39347

<http://www.securityfocus.com/bid/39347>

* SECTRACK: 1023853

<http://securitytracker.com/alerts/2010/Apr/1023853.html>

CVE Reference:

CVE-2010-0479 (cve.mitre.org, nvd.nist.gov)

• 18784 SMTP Server MX Record Vulnerability (MS10-024/981832) (Remote File Checking)

A denial of service vulnerability exists in the way that the Microsoft Windows Simple Mail Transfer Protocol (SMTP) component handles specially crafted DNS Mail Exchanger (MX) resource records. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted network message to a computer running the SMTP service. An attacker who successfully exploited this vulnerability could cause the SMTP service to stop responding until restarted.

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

References:

* VUPEN: VUPEN/ADV-2010-0867

<http://www.vupen.com/english/advisories/2010/0867>

* BID: 39308

<http://www.securityfocus.com/bid/39308>

* SECTRACK: 1023854

<http://securitytracker.com/alerts/2010/Apr/1023854.html>

* MS: MS10-024

<http://www.microsoft.com/technet/security/Bulletin/MS10-024.msp>

* CERT: TA10-103A

<http://www.us-cert.gov/cas/techalerts/TA10-103A.html>

CVE Reference:

CVE-2010-0024 (cve.mitre.org, nvd.nist.gov)

• 18785 SMTP Memory Allocation Vulnerability (MS10-024/981832) (Remote File Checking)

An information disclosure vulnerability exists in the Microsoft Windows Simple Mail Transfer Protocol (SMTP) component due to the manner in which the SMTP component handles memory allocation. An attacker could exploit the vulnerability by sending invalid commands, followed by the STARTTLS command, to an affected server. An attacker who successfully exploited this vulnerability could read random e-mail message fragments stored on the affected server. Note that this vulnerability would not allow an attacker to execute code or to elevate their user rights directly, but it could be used to produce useful information that could be used to try to further compromise the affected system.

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

References:

* VUPEN: VUPEN/ADV-2010-0867

<http://www.vupen.com/english/advisories/2010/0867>

* BID: 39381

<http://www.securityfocus.com/bid/39381>

* SECTRACK: 1023855

<http://securitytracker.com/alerts/2010/Apr/1023855.html>

* MS: MS10-024

<http://www.microsoft.com/technet/security/Bulletin/MS10-024.msp>

* CERT: TA10-103A

<http://www.us-cert.gov/cas/techalerts/TA10-103A.html>

* SECUNIA: 39253

<http://secunia.com/advisories/39253>

CVE Reference:

CVE-2010-0025 (cve.mitre.org, nvd.nist.gov)

• 18786 ISATAP IPv6 Source Address Spoofing Vulnerability (MS10-029/978338) (Remote File Checking)

A spoofing vulnerability exists in the Microsoft Windows IPv6 stack due to the way that Windows checks the inner packet's IPv6 source address in a tunneled ISATAP packet. An attacker who successfully exploited this vulnerability could impersonate an address to bypass edge or host firewalls. Additionally, information could be disclosed when the targeted computer replies to the message using the source IPv6 address that the attacker specified.

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

References:

* VUPEN: VUPEN/ADV-2010-0872

<http://www.vupen.com/english/advisories/2010/0872>

* BID: 39352

<http://www.securityfocus.com/bid/39352>

* SECTRACK: 1023857

<http://securitytracker.com/alerts/2010/Apr/1023857.html>

* MS: MS10-029

<http://www.microsoft.com/technet/security/Bulletin/MS10-029.msp>

* CERT: TA10-103A

<http://www.us-cert.gov/cas/techalerts/TA10-103A.html>

* SECUNIA: 39382

<http://secunia.com/advisories/39382>

CVE Reference:

CVE-2010-0812 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- CVE-2010-0772 IBM CVSS 2.0 Score = 4.0

Unspecified vulnerability in the channel process in IBM WebSphere MQ 7.0 before 7.0.1.2 allows remote authenticated users to cause a denial of service (daemon crash) via "incorrect channel control data."

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/58039>

CVE Reference: [CVE-2010-0772](#)

• **CVE-2010-1560 IBM CVSS 2.0 Score = 4.0**

Buffer overflow in the REPEAT function in IBM DB2 9.1 before FP9 allows remote authenticated users to cause a denial of service (trap) via unspecified vectors.

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

References:

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21426108>

VUPEN: <http://www.vupen.com/english/advisories/2010/0982>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg11C65922>

SECUNIA: <http://secunia.com/advisories/39500>

CVE Reference: [CVE-2010-1560](#)

• **CVE-2010-0105 Apple CVSS 2.0 Score = 4.9**

The hfs implementation in Apple Mac OS X 10.6.2 and 10.6.3 supports hard links to directories and does not prevent certain deeply nested directory structures, which allows local users to cause a denial of service (filesystem corruption) via a crafted application that calls the mkdir and link functions.

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

References:

BID: <http://www.securityfocus.com/bid/39658>

SREASONRES: http://securityreason.com/achievement_securityalert/83

CVE Reference: [CVE-2010-0105](#)

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