

2010 Issue #10

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

Threats you don't know about. Mariposa botnet operators arrested. Source code management a weak spot. Social networks and the workplace.

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

- **Underrated computing threats you need to know about**

Computerworld - There's the danger you know, and then there's the danger you don't know.

Most of us are rightfully wary of downloading and running programs that have no pedigree, or of performing day-to-day operations as an administrative user. But with each passing year, new security threats march in to eclipse the old — many of them not getting their share of attention until it's too late.

Threats go unappreciated for various reasons. Some seem too obscure or unlikely to be valid until they actually materialize in the wild (such as the .PDF exploits I document later on). Others are overshadowed by more widely publicized problems (e.g., the way Firefox's issues take a backseat to Internet Explorer's). Computerworld

Full Story :

http://www.computerworld.com/s/article/9164378/Underrated_computing_threats_you_need_to_know_about?source

- **Spain arrests three accused of running huge botnet**

Authorities in Spain have arrested three men accused of operating a massive botnet composed of 12.7 million PCs that stole credit card and bank log-in data and infected computers in half of the Fortune 1,000 companies and more than 40 banks, according to published reports.

The botnet "Mariposa," which means butterfly in Spanish, first appeared in December 2008 and grew to be one of the largest botnets ever, The Associated Press reported. It spread the Butterfly worm via removable drives, MSN Messenger, and peer-to-peer programs and targets Windows XP and older systems.

Unlike many underground hackers, the alleged ringleaders of the operation were not skilled programmers, but had contacts who were, authorities said. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-10462718-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• **Source code management a weak spot in Aurora attacks**

IDG News Service - Companies should take extra steps to secure their source code from the type of targeted attacks that hit Google, Adobe, Intel and others over the past few months.

That's according to security vendor McAfee, which released a report detailing the way software source code was accessed in some of these attacks. "We saw targeted attacks against software configuration management products," said George Kurtz, McAfee's chief technology officer.

In many of the attacks company engineers and technical staff were targeted with malicious software. And in some cases, source code management systems were accessed and code was downloaded outside of company firewalls, Kurtz said. Computerworld

Full Story :

http://www.computerworld.com/s/article/9165718/Source_code_management_a_weak_spot_in_Aurora_attacks?source=rss

• **Tweet this: Social network security is risky business**

Computerworld - SAN FRANCISCO -- Businesses are still trying to figure out what to make of social networking. The knee-jerk impulse at some companies is to ban its use because it's insecure and seen as unproductive, while at others it's viewed as, in fact, the way a lot of people now get work done.

The debate gets into familiar territory -- balancing business benefits versus risks -- and some that's not so familiar: Is a new generation in the workforce wired differently because of Facebook and Twitter?

"It starts way before college," said Gillian Hayes, a University of California at Irvine professor who took part in a panel at this week's RSA Security conference. "The emphasis is on 21st century skills, solving problems creatively; kids solve problems by mashing up bits and pieces." Computerworld

Full Story :

http://www.computerworld.com/s/article/9165778/Tweet_this_Social_network_security_is_risky_business?source=rss

New Vulnerabilities Tested in SecureScout

• **14540 Adobe Acrobat / Reader input validation Vulnerability (CVE-2009-2981) (Remote File Checking)**

Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 do not properly validate input, which might allow attackers to bypass intended Trust Manager restrictions via unspecified vectors.

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

References:

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb09-15.html>

* CERT: TA09-286B

<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>

* BID: 36638

<http://www.securityfocus.com/bid/36638>

* SECTRACK: 1023007

<http://securitytracker.com/id?1023007>

* VUPEN: ADV-2009-2898

<http://www.vupen.com/english/advisories/2009/2898>

CVE Reference:

CVE-2009-2981 (cve.mitre.org, nvd.nist.gov)

• **14541 Adobe Acrobat / Reader certificate Vulnerability (CVE-2009-2982) (Remote File Checking)**

An unspecified certificate in Adobe Reader and Acrobat 9.x before 9.2, 8.x before 8.1.7, and possibly 7.x through 7.1.4 might allow remote attackers to conduct a "social engineering attack" via unknown vectors.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb09-15.html>
- * CERT: TA09-286B
<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>
- * BID: 36638
<http://www.securityfocus.com/bid/36638>
- * SECTRACK: 1023007
<http://securitytracker.com/id?1023007>
- * VUPEN: ADV-2009-2898
<http://www.vupen.com/english/advisories/2009/2898>

CVE Reference:

CVE-2009-2982 (cve.mitre.org, nvd.nist.gov)

• **14542 Adobe Acrobat / Reader memory corruption Vulnerability (CVE-2009-2983) (Remote File Checking)**

Adobe Reader and Acrobat 9.x before 9.2, 8.x before 8.1.7, and possibly 7.x through 7.1.4 allow attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb09-15.html>
- * CERT: TA09-286B
<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>
- * BID: 36638
<http://www.securityfocus.com/bid/36638>
- * SECTRACK: 1023007
<http://securitytracker.com/id?1023007>
- * VUPEN: ADV-2009-2898
<http://www.vupen.com/english/advisories/2009/2898>

CVE Reference:

CVE-2009-2983 (cve.mitre.org, nvd.nist.gov)

• **14543 Adobe Acrobat image decoder Vulnerability (CVE-2009-2984) (Remote File Checking)**

Unspecified vulnerability in the image decoder in Adobe Acrobat 9.x before 9.2, and possibly 7.x through 7.1.4 and 8.x through 8.1.7, allows attackers to cause a denial of service or possibly execute arbitrary code via unknown vectors.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb09-15.html>
- * CERT: TA09-286B
<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>
- * BID: 36638
<http://www.securityfocus.com/bid/36638>
- * SECTRACK: 1023007
<http://securitytracker.com/id?1023007>
- * VUPEN: ADV-2009-2898
<http://www.vupen.com/english/advisories/2009/2898>

CVE Reference:

CVE-2009-2984 (cve.mitre.org, nvd.nist.gov)

● **14544 Adobe Acrobat / Reader memory corruption Vulnerability (CVE-2009-2985) (Remote File Checking)**

Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 allow attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2009-2996.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb09-15.html>
- * CERT: TA09-286B
<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>
- * BID: 36638
<http://www.securityfocus.com/bid/36638>
- * SECTRACK: 1023007
<http://securitytracker.com/id?1023007>
- * VUPEN: ADV-2009-2898
<http://www.vupen.com/english/advisories/2009/2898>

CVE Reference:

CVE-2009-2985 (cve.mitre.org, nvd.nist.gov)

● **14545 Adobe Acrobat / Reader multiple heap overflow Vulnerabilities (CVE-2009-2986) (Remote File Checking)**

Multiple heap-based buffer overflows in Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 might allow attackers to execute arbitrary code via unspecified vectors.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb09-15.html>
- * CERT: TA09-286B
<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>
- * BID: 36638
<http://www.securityfocus.com/bid/36638>
- * SECTRACK: 1023007
<http://securitytracker.com/id?1023007>
- * VUPEN: ADV-2009-2898
<http://www.vupen.com/english/advisories/2009/2898>

CVE Reference:

CVE-2009-2986 (cve.mitre.org, nvd.nist.gov)

● **14546 Adobe Acrobat / Reader remote denial of service Vulnerability (CVE-2009-2987) (Remote File Checking)**

Unspecified vulnerability in an ActiveX control in Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 on Windows allows remote attackers to cause a denial of service via unknown vectors.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb09-15.html>
- * CERT: TA09-286B
<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>
- * BID: 36638
<http://www.securityfocus.com/bid/36638>
- * SECTRACK: 1023007
<http://securitytracker.com/id?1023007>
- * VUPEN: ADV-2009-2898
<http://www.vupen.com/english/advisories/2009/2898>

CVE Reference:

CVE-2009-2987 (cve.mitre.org, nvd.nist.gov)

● **14547 Adobe Acrobat / Reader input validation Vulnerability (CVE-2009-2988) (Remote File Checking)**

Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 do not properly validate input, which allows attackers to cause a denial of service via unspecified vectors.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb09-15.html>
- * CERT: TA09-286B
<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>
- * BID: 36638
<http://www.securityfocus.com/bid/36638>
- * SECTRACK: 1023007
<http://securitytracker.com/id?1023007>
- * VUPEN: ADV-2009-2898
<http://www.vupen.com/english/advisories/2009/2898>

CVE Reference:

CVE-2009-2988 (cve.mitre.org, nvd.nist.gov)

● **14548 Adobe Acrobat / Reader integer overflow Vulnerability (CVE-2009-2989) (Remote File Checking)**

Integer overflow in Adobe Acrobat 9.x before 9.2, 8.x before 8.1.7, and possibly 7.x through 7.1.4 might allow attackers to execute arbitrary code via unspecified vectors.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb09-15.html>
- * CERT: TA09-286B
<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>
- * BID: 36638
<http://www.securityfocus.com/bid/36638>
- * SECTRACK: 1023007
<http://securitytracker.com/id?1023007>
- * VUPEN: ADV-2009-2898
<http://www.vupen.com/english/advisories/2009/2898>

CVE Reference:

CVE-2009-2989 (cve.mitre.org, nvd.nist.gov)

● **14549 Adobe Acrobat / Reader Array index error Vulnerability (CVE-2009-2990) (Remote File Checking)**

Array index error in Adobe Reader and Acrobat 9.x before 9.2, 8.x before 8.1.7, and possibly 7.x through 7.1.4 might allow attackers to execute arbitrary code via unspecified vectors.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb09-15.html>
- * CERT: TA09-286B
<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>
- * BID: 36638
<http://www.securityfocus.com/bid/36638>
- * SECTRACK: 1023007
<http://securitytracker.com/id?1023007>
- * VUPEN: ADV-2009-2898
<http://www.vupen.com/english/advisories/2009/2898>

CVE Reference:

CVE-2009-2990 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-0483 Microsoft CVSS 2.0 Score = 7.6

VBScript in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2, when Internet Explorer is used, allows user-assisted remote attackers to execute arbitrary code by referencing a (1) local pathname, (2) UNC share pathname, or (3) WebDAV server with a crafted .hlp file in the fourth argument (aka helpfile argument) to the MsgBox function, leading to code execution involving winhlp32.exe when the F1 key is pressed.

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

References:

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

MISC: https://www.metasploit.com/svn/framework3/trunk/modules/exploits/windows/browser/ie_winhlp32.rb

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

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

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

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

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

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

MISC:

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

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

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

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

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

CONFIRM:

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

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

CONFIRM:

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

CVE Reference: [CVE-2010-0483](#)

• CVE-2010-0917 Microsoft CVSS 2.0 Score = 7.6

Stack-based buffer overflow in VBScript in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2, when Internet Explorer is used, might allow user-assisted remote attackers to execute arbitrary code via a long string in the fourth argument (aka helpfile argument) to the MsgBox function, leading to code execution when the F1 key is pressed, a different vulnerability than CVE-2010-0483.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/56560>

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

BID: <http://www.securityfocus.com/bid/38473>

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

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

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

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

CVE Reference: [CVE-2010-0917](#)

• **CVE-2010-0918 IBM CVSS 2.0 Score = 10.0**

Multiple unspecified vulnerabilities in the UltraLite functionality in IBM Lotus iNotes (aka Domino Web Access or DWA) before 229.281 for Domino 8.0.2 FP4 have unknown impact and attack vectors.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/56557>

VUPEN: <http://www.vupen.com/english/advisories/2010/0496>

BID: <http://www.securityfocus.com/bid/38459>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27018109>

CVE Reference: [CVE-2010-0918](#)

• **CVE-2010-0922 IBM CVSS 2.0 Score = 7.8**

Unspecified vulnerability in secdaplntd in IBM AIX 5.3 with SP 5300-11-02 allows attackers to cause a denial of service (LDAP login failure) via unknown vectors. NOTE: some of these details are obtained from third party information. NOTE: there may be no attacker role, and the issue may be triggered entirely by an administrator's installation of an official service pack.

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

References:

CONFIRM: <http://www14.software.ibm.com/webapp/set2/subscriptions/pqvcmjd?mode=18&ID=4956>

BID: <http://www.securityfocus.com/bid/38444>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ69977>

CONFIRM: <ftp://public.dhe.ibm.com/aix/efixes/iz69977/README.txt>

CVE Reference: [CVE-2010-0922](#)

• **CVE-2010-0919 IBM CVSS 2.0 Score = 7.6**

Stack-based buffer overflow in the Lotus Domino Web Access ActiveX control in IBM Lotus iNotes (aka Domino Web Access or DWA) 6.5, 7.0 before 7.0.4, 8.0, 8.0.2, and before 229.281 for Domino 8.0.2 FP4 allows remote attackers to execute arbitrary code via a long URL argument to an unspecified method, aka PRAD7JTNHJ.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/0496>

XF: <http://xforce.iss.net/xforce/xfdb/56555>

VUPEN: <http://www.vupen.com/english/advisories/2010/0495>

BID: <http://www.securityfocus.com/bid/38459>

BID: <http://www.securityfocus.com/bid/38457>

OSVDB: <http://www.osvdb.org/62612>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27018109>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21421808>

SECTRACK: <http://securitytracker.com/id?1023662>

SECUNIA: <http://secunia.com/advisories/38755>

SECUNIA: <http://secunia.com/advisories/38744>

SECUNIA: <http://secunia.com/advisories/38681>

IDEFENSE: <http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=857>

CVE Reference: [CVE-2010-0919](#)

• **CVE-2010-0921 IBM CVSS 2.0 Score = 6.8**

Cross-site request forgery (CSRF) vulnerability in IBM Lotus iNotes (aka Domino Web Access or DWA) before 229.281 for Domino 8.0.2 FP4 allows remote attackers to hijack the authentication of unspecified victims via vectors related to lack of "XSS/CSRF Get Filter and Referer Check fixes."

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/56556>

VUPEN: <http://www.vupen.com/english/advisories/2010/0496>

BID: <http://www.securityfocus.com/bid/38459>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27018109>

CVE Reference: [CVE-2010-0921](#)

• **CVE-2010-0920 IBM CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in IBM Lotus iNotes (aka Domino Web Access or DWA) before 229.281 for Domino 8.0.2 FP4 allows remote attackers to inject arbitrary web script or HTML via vectors related to lack of "XSS/CSRF Get Filter and Referer Check fixes."

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/0496>

BID: <http://www.securityfocus.com/bid/38459>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27018109>

CVE Reference: [CVE-2010-0920](#)

• **CVE-2010-0924 Apple CVSS 2.0 Score = 5.0**

cfnetwork.dll 1.450.5.0 in CFNetwork, as used by safari.exe 531.21.10 in Apple Safari 4.0.3 and 4.0.4 on Windows, allows remote attackers to cause a denial of service (application crash) via a long string in the BACKGROUND attribute of a BODY element.

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

References:

BID: <http://www.securityfocus.com/bid/38447>

MISC: http://nobytes.com/exploits/Safari_4.0.4_background_DoS_pl.txt

CVE Reference: [CVE-2010-0924](#)

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