

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

Security guide from ISACA. Cyber Security Awareness Month is here. Stuxnet causes worries. Data breach from payment terminals.

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

• Nonprofit releases new security guidance

The Information Systems Audit and Control Association (ISACA), a nonprofit association of information security, assurance and IT governance professionals, on Wednesday issued a new guidance document outlining a business model for information security. The document is the result of two years of research and expert review and is intended to provide a blueprint to align security projects with business strategy, said Rolf von Roessing, international vice president of ISACA. The technology-neutral model addresses various aspects of IT and privacy and is applicable across industries, countries and regulatory and legal systems. ISACA members can receive the full document for free and nonmembers can receive an introductory guide at no cost. - AM SC Magazine

Full Story :

http://www.scmagazineus.com/nonprofit-releases-new-security-guidance/article/180550/?utm_source=feedburner&utm_medium=feed&utm_campaign=story_mail

• Keeping the masses safe on the Internet

SANTA CLARA, Calif.--Recognizing that all the technology in the world can't protect the Internet from attacks, the security industry is targeting an education campaign at the weakest link--the computer users.

It's the first public service message of its kind in the U.S. and it's simple: Stop. Think. Connect.

The campaign was unveiled yesterday at Intel headquarters here. It is part of Cyber Security Awareness Month, an annual event since October 2001, and was organized by the National Cyber Security Alliance, the Anti-Phishing Working Group (APWG) and more than two dozen government agencies and companies including Microsoft, Google, PayPal, RSA, Facebook, Visa, and Wal-Mart. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20018842-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• More than half of critical infrastructure targeted

In the wake of the Stuxnet worm, which targeted industrial control systems around the world and caused serious concern about the threat of cyberwarfare, a new survey found that 53 percent of critical infrastructure providers said their networks have experienced politically motivated attacks. The survey of 1,580 private, critical infrastructure businesses from 15 countries worldwide, released Wednesday by Symantec, also found that 48 percent of respondents suspect they will suffer politically motivated attacks in the future. Of those that already have been hit, companies typically reported sustaining about 10 attacks in the past five years, according to the report.

The Stuxnet worm is an example that politically motivated attacks, while uncommon, are real and can be effective, Cris Paden, a Symantec spokesman, told SCMagazineUS.com on Thursday. SC Magazine

Full Story :

http://www.scmagazineus.com/more-than-half-of-critical-infrastructure-targeted/article/180590/?utm_source=feedburn

• Aldi data breach shows payment terminal holes

Computerworld - A debit card breach disclosed late last week by discount grocer Aldi Inc. shows how hardware hacks are starting to pose as much of a threat to payment card data as software-based attacks.

Batavia, Ill.-based Aldi, which operates 1,100 stores in 31 states, disclosed on Oct. 1 that hackers tampered with payment terminals at stores in 11 states from June to August.

The hackers gained access to various debit card data, such as name, account data and personal identification numbers (PINs) of an undisclosed number of customers, the company said. Computerworld

Full Story :

http://www.computerworld.com/s/article/9189982/Aldi_data_breach_shows_payment_terminal_holes?source=rss_sec

New Vulnerabilities Tested in SecureScout

• 14596 Adobe Acrobat / Reader font-parsing input validation Vulnerability (Remote File Checking)

Stack-based buffer overflow in CoolType.dll in Adobe Reader and Acrobat 9.3.4 and earlier allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a PDF document with a long field in a Smart INdependent Glyphlets (SING) table in a TTF font, as exploited in the wild in September 2010. NOTE: some of these details are obtained from third party information.

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

References:

* MISC:

<http://blog.metasploit.com/2010/09/return-of-unpublished-adobe.html>

* MISC:

<http://community.websense.com/blogs/securitylabs/archive/2010/09/10/brief-analysis-on-adobe-reader-sing-table-parsing->

* CONFIRM:

<http://www.adobe.com/support/security/advisories/apsa10-02.html>

* CERT-VN: VU#491991

<http://www.kb.cert.org/vuls/id/491991>

* BID: 43057

<http://www.securityfocus.com/bid/43057>

* SECUNIA: 41340

<http://secunia.com/advisories/41340>

* VUPEN: ADV-2010-2331

<http://www.vupen.com/english/advisories/2010/2331>

* XF: adobe-reader-cooltype-code-execution(61635)

<http://xforce.iss.net/xforce/xfdb/61635>

CVE Reference:

CVE-2010-2883 (cve.mitre.org, nvd.nist.gov)

• **14597 Adobe Acrobat / Reader memory corruption in the authplay.dll Vulnerability (Remote File Checking)**

Unspecified vulnerability in Adobe Flash Player 10.1.82.76 and earlier for Windows, Macintosh, Linux, Solaris; Flash Player 10.1.92.10 for Android; Reader 9.3.4 for Windows, Macintosh and UNIX; and Acrobat 9.3.4 and earlier for Windows and Macintosh allows remote attackers to cause a denial of service (crash) and execute arbitrary code via unknown vectors, as exploited in the wild in September 2010.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/advisories/apsa10-03.html>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb10-22.html>
- * REDHAT: RHSA-2010:0706
<http://www.redhat.com/support/errata/RHSA-2010-0706.html>
- * CERT: TA10-263A
<http://www.us-cert.gov/cas/techalerts/TA10-263A.html>
- * CERT-VN: VU#275289
<http://www.kb.cert.org/vuls/id/275289>
- * SECUNIA: 41434
<http://secunia.com/advisories/41434>
- * SECUNIA: 41435
<http://secunia.com/advisories/41435>
- * SECUNIA: 41443
<http://secunia.com/advisories/41443>
- * SECUNIA: 41526
<http://secunia.com/advisories/41526>
- * VUPEN: ADV-2010-2348
<http://www.vupen.com/english/advisories/2010/2348>
- * VUPEN: ADV-2010-2349
<http://www.vupen.com/english/advisories/2010/2349>
- * XF: adobe-flash-content-code-execution(61771)
<http://xforce.iss.net/xforce/xfdb/61771>

CVE Reference:

CVE-2010-2884 (cve.mitre.org, nvd.nist.gov)

• **14598 Adobe Acrobat / Reader multiple input validation errors that could lead to code execution Vulnerability (Remote File Checking)**

Multiple unspecified vulnerabilities in an ActiveX control in Adobe Reader and Acrobat 8.x before 8.2.5 and 9.x before 9.4 on Windows allow attackers to execute arbitrary code via unknown vectors.

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

References:

- * VUPEN: VUPEN/ADV-2010-2573
<http://www.vupen.com/english/advisories/2010/2573>
- * SECTRACK: 1024511
<http://securitytracker.com/alerts/2010/Oct/1024511.html>
- * BID: 43739
<http://www.securityfocus.com/bid/43739>
- * CONFIRM: apsb10-21
<http://www.adobe.com/support/security/bulletins/apsb10-21.html>

CVE Reference:

CVE-2010-2888 (cve.mitre.org, nvd.nist.gov)

• **14599 Adobe Acrobat / Reader font-parsing input validation Vulnerability (CVE-2010-2889) (Remote File Checking)**

Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allows attackers to execute arbitrary code via a crafted font, a different vulnerability than CVE-2010-3626.

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

References:

- * VUPEN: VUPEN/ADV-2010-2573
<http://www.vupen.com/english/advisories/2010/2573>
- * SECTRACK: 1024511
<http://securitytracker.com/alerts/2010/Oct/1024511.html>
- * BID: 43723
<http://www.securityfocus.com/bid/43723>
- * CONFIRM: apsb10-21
<http://www.adobe.com/support/security/bulletins/apsb10-21.html>

CVE Reference:

CVE-2010-2889 (cve.mitre.org, nvd.nist.gov)

• **14600 Adobe Acrobat / Reader memory corruption Vulnerability (Remote File Checking)**

Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-3619, CVE-2010-3621, CVE-2010-3622, CVE-2010-3628, CVE-2010-3632, and CVE-2010-3658.

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

References:

- * VUPEN: VUPEN/ADV-2010-2573
<http://www.vupen.com/english/advisories/2010/2573>
- * SECTRACK: 1024511
<http://securitytracker.com/alerts/2010/Oct/1024511.html>
- * BID: 43722
<http://www.securityfocus.com/bid/43722>
- * CONFIRM: apsb10-21
<http://www.adobe.com/support/security/bulletins/apsb10-21.html>

CVE Reference:

CVE-2010-2890 (cve.mitre.org, nvd.nist.gov)

• **14601 Adobe Acrobat / Reader memory corruption Vulnerability (CVE-2010-3619) (Remote File Checking)**

Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-2890, CVE-2010-3621, CVE-2010-3622, CVE-2010-3628, CVE-2010-3632, and CVE-2010-3658.

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

References:

- * VUPEN: VUPEN/ADV-2010-2573
<http://www.vupen.com/english/advisories/2010/2573>
- * SECTRACK: 1024511
<http://securitytracker.com/alerts/2010/Oct/1024511.html>
- * BID: 43724
<http://www.securityfocus.com/bid/43724>
- * CONFIRM: apsb10-21
<http://www.adobe.com/support/security/bulletins/apsb10-21.html>

CVE Reference:

CVE-2010-3619 (cve.mitre.org, nvd.nist.gov)

• **14602 Adobe Acrobat / Reader image-parsing input validation Vulnerability (Remote File Checking)**

Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allows attackers to execute arbitrary code via a crafted image, a different vulnerability than CVE-2010-3629.

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

References:

* VUPEN: VUPEN/ADV-2010-2573
<http://www.vupen.com/english/advisories/2010/2573>
* SECTRACK: 1024511
<http://securitytracker.com/alerts/2010/Oct/1024511.html>
* BID: 43725
<http://www.securityfocus.com/bid/43725>
* CONFIRM: apsb10-21
<http://www.adobe.com/support/security/bulletins/apsb10-21.html>

CVE Reference:

CVE-2010-3620 (cve.mitre.org, nvd.nist.gov)

• **14603 Adobe Acrobat / Reader memory corruption Vulnerability (CVE-2010-3621) (Remote File Checking)**

Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-2890, CVE-2010-3619, CVE-2010-3622, CVE-2010-3628, CVE-2010-3632, and CVE-2010-3658.

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

References:

* VUPEN: VUPEN/ADV-2010-2573
<http://www.vupen.com/english/advisories/2010/2573>
* SECTRACK: 1024511
<http://securitytracker.com/alerts/2010/Oct/1024511.html>
* BID: 43726
<http://www.securityfocus.com/bid/43726>
* CONFIRM: apsb10-21
<http://www.adobe.com/support/security/bulletins/apsb10-21.html>

CVE Reference:

CVE-2010-3621 (cve.mitre.org, nvd.nist.gov)

• **14604 Adobe Acrobat / Reader memory corruption Vulnerability (CVE-2010-3622) (Remote File Checking)**

Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-2890, CVE-2010-3619, CVE-2010-3621, CVE-2010-3628, CVE-2010-3632, and CVE-2010-3658.

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

References:

* VUPEN: VUPEN/ADV-2010-2573
<http://www.vupen.com/english/advisories/2010/2573>
* SECTRACK: 1024511
<http://securitytracker.com/alerts/2010/Oct/1024511.html>
* BID: 43729
<http://www.securityfocus.com/bid/43729>
* CONFIRM: apsb10-21
<http://www.adobe.com/support/security/bulletins/apsb10-21.html>

CVE Reference:

CVE-2010-3622 (cve.mitre.org, nvd.nist.gov)

• **14605 Adobe Acrobat / Reader prefix protocol handler Vulnerability (Remote File Checking)**

Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allow attackers to execute arbitrary code via unspecified vectors, related to a "prefix protocol handler vulnerability."

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

References:

* VUPEN: VUPEN/ADV-2010-2573
<http://www.vupen.com/english/advisories/2010/2573>
* SECTRACK: 1024511

<http://securitytracker.com/alerts/2010/Oct/1024511.html>

* BID: 43730

<http://www.securityfocus.com/bid/43730>

* CONFIRM: apsb10-21

<http://www.adobe.com/support/security/bulletins/apsb10-21.html>

CVE Reference:

CVE-2010-3625 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-3315 Apache CVSS 2.0 Score = 6.0

authz.c in the mod_dav_svn module for the Apache HTTP Server, as distributed in Apache Subversion 1.5.x before 1.5.8 and 1.6.x before 1.6.13, when SVNPathAuthz short_circuit is enabled, does not properly handle a named repository as a rule scope, which allows remote authenticated users to bypass intended access restrictions via svn commands.

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

References:

CONFIRM: <http://subversion.apache.org/security/CVE-2010-3315-advisory.txt>

CONFIRM: <http://security-tracker.debian.org/tracker/CVE-2010-3315>

SECUNIA: <http://secunia.com/advisories/41652>

CVE Reference: [CVE-2010-3315](http://cve.mitre.org/cve/2010/3315)

• CVE-2010-1623 Apache CVSS 2.0 Score = 5.0

The apr_brigade_split_line function in buckets/apr_brigade.c in the Apache Portable Runtime Utility library (aka APR-util) before 1.3.10, as used in the mod_reqtimeout module in the Apache HTTP Server and other software, allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/2556>

CONFIRM: <http://svn.apache.org/viewvc?view=revision&revision=1003626>

CONFIRM: <http://svn.apache.org/viewvc?view=revision&revision=1003495>

CONFIRM: <http://svn.apache.org/viewvc?view=revision&revision=1003494>

CONFIRM: <http://svn.apache.org/viewvc?view=revision&revision=1003493>

CONFIRM: <http://svn.apache.org/viewvc?view=revision&revision=1003492>

VUPEN: <http://www.vupen.com/english/advisories/2010/2557>

BID: <http://www.securityfocus.com/bid/43673>

MANDRIVA: <http://www.mandriva.com/security/advisories?name=MDVSA-2010:192>

CONFIRM: <http://www.apache.org/dist/apr/CHANGES-APR-UTIL-1.3>

CONFIRM: <http://security-tracker.debian.org/tracker/CVE-2010-1623>

SECUNIA: <http://secunia.com/advisories/41701>

CVE Reference: [CVE-2010-1623](http://cve.mitre.org/cve/2010/1623)

• CVE-2010-3731 IBM CVSS 2.0 Score = 10.0

Buffer overflow in the Administration Server component in IBM DB2 UDB 9.5 before FP6a allows remote attackers to cause a denial of service or possibly execute arbitrary code via unspecified vectors. NOTE: some of these details are obtained from third party information.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/2544>

SECUNIA: <http://secunia.com/advisories/41686>

CONFIRM: ftp://public.dhe.ibm.com/ps/products/db2/fixes/english-us/aparlist/db2_v95/APARLIST.TXT

CVE Reference: [CVE-2010-3731](#)

• **CVE-2010-3733 IBM CVSS 2.0 Score = 7.2**

The Engine Utilities component in IBM DB2 UDB 9.5 before FP6a uses world-writable permissions for the sqllib/cfg/db2sprf file, which might allow local users to gain privileges by modifying this file.

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

References:

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg11Z68463>

CONFIRM: ftp://public.dhe.ibm.com/ps/products/db2/fixes/english-us/aparlist/db2_v95/APARLIST.TXT

CVE Reference: [CVE-2010-3733](#)

• **CVE-2010-3739 IBM CVSS 2.0 Score = 6.4**

The audit facility in the Security component in IBM DB2 UDB 9.5 before FP6a uses instance-level audit settings to capture connection (aka CONNECT and AUTHENTICATION) events in certain circumstances in which database-level audit settings were intended, which might make it easier for remote attackers to connect without discovery.

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

References:

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1JR34218>

CONFIRM: ftp://public.dhe.ibm.com/ps/products/db2/fixes/english-us/aparlist/db2_v95/APARLIST.TXT

CVE Reference: [CVE-2010-3739](#)

• **CVE-2010-3734 IBM CVSS 2.0 Score = 5.0**

The Install component in IBM DB2 UDB 9.5 before FP6a on Linux, UNIX, and Windows enforces an unintended limit on password length, which makes it easier for attackers to obtain access via a brute-force attack.

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

References:

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg11C62856>

CONFIRM: ftp://public.dhe.ibm.com/ps/products/db2/fixes/english-us/aparlist/db2_v95/APARLIST.TXT

CVE Reference: [CVE-2010-3734](#)

• **CVE-2010-3738 IBM CVSS 2.0 Score = 5.0**

The Security component in IBM DB2 UDB 9.5 before FP6a logs AUDIT events by using a USERID and an AUTHID value corresponding to the instance owner, instead of a USERID and an AUTHID value corresponding to the logged-in user account, which makes it easier for remote authenticated users to execute Audit administration commands without discovery.

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

References:

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg11C65184>

CONFIRM: ftp://public.dhe.ibm.com/ps/products/db2/fixes/english-us/aparlist/db2_v95/APARLIST.TXT

CVE Reference: [CVE-2010-3738](#)

• **CVE-2010-3736 IBM CVSS 2.0 Score = 4.0**

Memory leak in the Relational Data Services component in IBM DB2 UDB 9.5 before FP6a, when the connection concentrator is enabled, allows remote authenticated users to cause a denial of service (heap memory consumption) by using a different code page than the database server.

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

References:

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg11C68182>

CONFIRM: ftp://public.dhe.ibm.com/ps/products/db2/fixes/english-us/aparlist/db2_v95/APARLIST.TXT

CVE Reference: [CVE-2010-3736](https://cve.mitre.org/cve/2010/3736)

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