ScoutNews
The weekly Security update from the makers of SecureScout
February 26, 2010

2010 Issue #9

Table of Contents

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

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

2009 vulns and attacks report. Domains shut down by judge. RSA 2010 on crime, cloud and consumerization. Cyber attacks can lead to catastrophe.

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

- **IBM report: Vulnerabilities fell in '09, attacks rose**

The 2009 cybersecurity landscape had its peaks and its valleys - the number of new and unpatched vulnerabilities decreased compared to 2008, but attack volume grew substantially, according to a research report from IBM ISS released on Thursday. There were 6,601 new vulnerabilities discovered last year, an 11 percent decrease compared to 2008, according to the annual "X-Force Trend and Risk Report." In addition, the number of vulnerabilities in web browsers and document readers with no patch also decreased last year compared to 2008. And, the number of unpatched "critical" vulnerabilities is significantly lower than years past, indicating that software vendors have become more responsive when dealing with security issues, the report stated.

"The computer industry is getting better at building secure software and being responsive to vulnerabilities," Tom Cross, manager of IBM X-Force Research, told SCMagazineUS.com on Thursday. "But the volume of attack activity is expanding at a very rapid pace." SC Magazine

Full Story :
http://www.scmagazineus.com/ibm-report-vulnerabilities-fell-in-09-attacks-rose/article/164547/?utm_source=feedbur

- **Waledac demise imminent after shutdown of domains**

A federal judge this week ordered the takedown of nearly 300 domains being used to provide instructions to malware-infected computers, a move that effectively incapacitates Waledac, one of the most prolific botnets of all time.

The judge, sitting in U.S. District Court in Alexandra, Va., was responding to a lawsuit filed by Microsoft that asked the court to grant a temporary restraining order to cut off 277 domains being run by the operators of Waledac. The botnet, which began appearing at the end of 2008 as a kind of replacement for the Storm worm, is believed to have infected hundreds of thousands of PCs globally. SC Magazine

Full Story :
http://www.scmagazineus.com/waledac-demise-imminent-after-shutdown-of-domains/article/164535/?utm_source=fe

- **Crime, cloud and consumerization on tap at RSA 2010**

What should IT personnel and executives at enterprises know before adopting a cloud computing model? How are CISOs dealing with the trend of consumerization? How will mobile app stores affect the threat environment?

These questions and more will be addressed at the 2010 RSA Conference, being held Monday through March 5 at the Moscone Center in San Francisco.

Three of the main themes that will drive this year's conference are cybercrime, cloud computing and consumerization, according to industry analysts who participated in a pre-show teleconference on Wednesday. SC Magazine

Full Story :
http://www.scmagazineus.com/crime-cloud-and-consumerization-on-tap-at-rsa-2010/article/164442/?utm_source=fee

- **Experts warn of catastrophe from cyberattacks**

Vice Admiral Michael McConnell, who works for Booz Allen Hamilton and used to be director of national security and intelligence for the U.S. government.

(Credit: U.S. Senate)

Computer-based network attacks are slowly bleeding U.S. businesses of revenue and market advantage, while the government faces the prospect of losing in an all-out cyberwar, experts told Senators in a hearing on Tuesday. Cnet Security

Full Story :
http://news.cnet.com/8301-27080_3-10458759-245.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

- **14535 Adobe Acrobat / Reader Denial of Service Vulnerability (CVE-2010-0188) (Remote File Checking)**

A critical vulnerability (CVE-2010-0188) has been identified that could cause the application to crash and could potentially allow an attacker to take control of the affected system.

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

References:

* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb10-07.html
* REDHAT: RHSA-2010:0114
http://www.redhat.com/support/errata/RHSA-2010-0114.html
* BID: 38195
http://www.securityfocus.com/bid/38195
* SECTRACK: 1023601
http://securitytracker.com/id?1023601
* VUPEN: ADV-2010-0399

http://www.vupen.com/english/advisories/2010/0399
* XF: adobe-unspec-priv-escalation(56297)
http://xforce.iss.net/xforce/xfdb/56297

CVE Reference:

CVE-2010-0188 (cve.mitre.org, nvd.nist.gov)

• 14536 Adobe Acrobat / Reader cross-domain requests Vulnerability (CVE-2010-0186) (Remote File Checking)

A critical vulnerability has been identified in Adobe Reader 9.3 for Windows, Macintosh and UNIX, Adobe Acrobat 9.3 for Windows and Macintosh, and Adobe Reader 8.2 and Acrobat 8.2 for Windows and Macintosh. As described in Security Bulletin APSB10-06, this vulnerability (CVE-2010-0186) could subvert the domain sandbox and make unauthorized cross-domain requests.

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

References:

* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb10-06.html
* CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=563819
* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb10-07.html
* REDHAT: RHSA-2010:0102
https://rhn.redhat.com/errata/RHSA-2010-0102.html
* REDHAT: RHSA-2010:0103
https://rhn.redhat.com/errata/RHSA-2010-0103.html
* REDHAT: RHSA-2010:0114
http://www.redhat.com/support/errata/RHSA-2010-0114.html
* BID: 38198
http://www.securityfocus.com/bid/38198
* OSVDB: 62300
http://www.osvdb.org/62300
* SECTRACK: 1023585
http://securitytracker.com/id?1023585

CVE Reference:

CVE-2010-0186 (cve.mitre.org, nvd.nist.gov)

• 14537 Adobe Acrobat / Reader memory corruption Vulnerability (CVE-2009-1862) (Remote File Checking)

Unspecified vulnerability in Adobe Reader and Acrobat 9.x through 9.1.2, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via (1) a crafted Flash application in a .pdf file or (2) a crafted .swf file, related to authplay.dll, as exploited in the wild in July 2009.

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

References:

* MISC:
http://blogs.adobe.com/psirt/2009/07/potential_adobe_reader_and_fla.html
* MISC:
http://bugs.adobe.com/jira/browse/FP-1265
* MISC:
http://isc.sans.org/diary.html?storyid=6847
* MISC:
http://news.cnet.com/8301-27080_3-10293389-245.html
* MISC:
http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-072209-2512-99
* MISC:
http://www.symantec.com/connect/blogs/next-generation-flash-vulnerability
* CONFIRM:
http://www.adobe.com/support/security/advisories/apsa09-03.html
* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb09-13.html
* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb09-10.html
* CONFIRM:

http://support.apple.com/kb/HT3864
* CONFIRM:
http://support.apple.com/kb/HT3865
* APPLE: APPLE-SA-2009-09-10-1
http://lists.apple.com/archives/security-announce/2009/Sep/msg00003.html
* APPLE: APPLE-SA-2009-09-10-2
http://lists.apple.com/archives/security-announce/2009/Sep/msg00004.html
* GENTOO: GLSA-200908-04
http://security.gentoo.org/glsa/glsa-200908-04.xml
* SUNALERT: 266108
http://sunsolve.sun.com/search/document.do?assetkey=1-66-266108-1
* CERT-VN: VU#259425
http://www.kb.cert.org/vuls/id/259425
* BID: 35759
http://www.securityfocus.com/bid/35759
* SECUNIA: 36193
http://secunia.com/advisories/36193
* SECUNIA: 36374
http://secunia.com/advisories/36374
* SECUNIA: 36701
http://secunia.com/advisories/36701

CVE Reference:

CVE-2009-1862 (cve.mitre.org, nvd.nist.gov)

• 14538 Adobe Acrobat / Reader XMP-XML entity expansion Vulnerability (CVE-2009-2979) (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 do not properly perform XMP-XML entity expansion, which allows remote attackers to cause a denial of service via a crafted document.

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-2009-2979 (cve.mitre.org, nvd.nist.gov)

• 14539 Adobe Acrobat / Reader Integer overflow Vulnerability (CVE-2009-2980) (Remote File Checking)

Integer overflow in Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 allows attackers to cause a denial of service 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-2009-2980 (cve.mitre.org, nvd.nist.gov)

- **18716 MSO.DLL Buffer Overflow (MS10-003/978214) (Remote File Checking)**

A remote code execution vulnerability exists in the way Microsoft Office handles specially crafted Office files. 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:

* BID: 38073
http://www.securityfocus.com/bid/38073
* VUPEN: VUPEN/ADV-2010-0336
http://www.vupen.com/english/advisories/2010/0336
* SECTRACK: 1023565
http://securitytracker.com/alerts/2010/Feb/1023565.html
* MS: MS10-003
http://www.microsoft.com/technet/security/Bulletin/MS10-003.mspx

CVE Reference:

CVE-2010-0243 (cve.mitre.org, nvd.nist.gov)

- **18717 Hyper-V Instruction Set Validation Vulnerability (MS10-010/977894) (Remote File Checking)**

A denial of service vulnerability exists in Hyper-V on Windows Server 2008 and Windows Server 2008 R2. The vulnerability is due to insufficient validation of specific sequences of machine instructions by Hyper-V. An attacker who successfully exploited this vulnerability could cause the affected Hyper-V system to stop responding. This would affect all virtual machines hosted by that system.

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

References:

* BID: 38113
http://www.securityfocus.com/bid/38113
* VUPEN: VUPEN/ADV-2010-0343
http://www.vupen.com/english/advisories/2010/0343
* SECTRACK: 1023567
http://securitytracker.com/alerts/2010/Feb/1023567.html
* MS: MS10-010
http://www.microsoft.com/technet/security/Bulletin/MS10-010.mspx

CVE Reference:

CVE-2010-0026 (cve.mitre.org, nvd.nist.gov)

- **18718 CSRSS Local Privilege Elevation Vulnerability (MS10-011/978037) (Remote File Checking)**

An elevation of privilege vulnerability exists because the Windows Client/Server Run-time Subsystem (CSRSS) does not properly terminate user processes when a user logs out. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

* BID: 38098
http://www.securityfocus.com/bid/38098
* VUPEN: VUPEN/ADV-2010-0344
http://www.vupen.com/english/advisories/2010/0344
* SECTRACK: 1023569
http://securitytracker.com/alerts/2010/Feb/1023569.html
* MS: MS10-011
http://www.microsoft.com/technet/security/Bulletin/MS10-011.mspx

CVE Reference:

CVE-2010-0023 (cve.mitre.org, nvd.nist.gov)

- **18719 Kerberos Null Pointer Dereference Vulnerability (MS10-014/977290) (Remote File Checking)**

A denial of service vulnerability exists in implementations of Kerberos. The vulnerability is due to improper handling of Ticket-Granting-Ticket renewal requests by a client on a remote, non-Windows realm in a mixed-mode Kerberos implementation. An attacker who successfully exploited this vulnerability could cause the affected Windows domain controller to stop responding.

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

References:

* BID: 38110
http://www.securityfocus.com/bid/38110
* VUPEN: VUPEN/ADV-2010-0347
http://www.vupen.com/english/advisories/2010/0347
* SECTRACK: 1023566
http://securitytracker.com/alerts/2010/Feb/1023566.html
* MS: MS10-014
http://www.microsoft.com/technet/security/Bulletin/MS10-014.mspx

CVE Reference:

CVE-2010-0035 (cve.mitre.org, nvd.nist.gov)

- **18720 MS Paint Integer Overflow Vulnerability (MS10-005/978706) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Paint decodes JPEG images. The vulnerability could allow remote code execution if a user opens a specially crafted JPEG image file in Microsoft Paint. 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.

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

References:

* BID: 38042
http://www.securityfocus.com/bid/38042
* VUPEN: VUPEN/ADV-2010-0338
http://www.vupen.com/english/advisories/2010/0338
* SECTRACK: 1023564
http://securitytracker.com/alerts/2010/Feb/1023564.html
* MS: MS10-005
http://www.microsoft.com/technet/security/Bulletin/MS10-005.mspx
* SECUNIA: 36634
http://secunia.com/advisories/36634

CVE Reference:

CVE-2010-0028 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- **CVE-2010-0719 Microsoft CVSS 2.0 Score = 4.7**

An unspecified API in Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 does not validate arguments, which allows local users to cause a denial of service (system crash) via a crafted application.

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

References:

MISC: http://www.scmagazineus.com/malta-researchers-find-windows-bug-that-crashes-pcs/article/164439/

SECTRACK: http://securitytracker.com/id?1023656

CVE Reference: CVE-2010-0719

- **CVE-2010-0718 Microsoft CVSS 2.0 Score = 4.3**

Buffer overflow in Microsoft Windows Media Player 9 and 11.0.5721.5145 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted .mpg file.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/56435

MISC: http://www.exploit-db.com/exploits/11531

CVE Reference: CVE-2010-0718

- **CVE-2010-0716 Microsoft CVSS 2.0 Score = 3.5**

_layouts/Upload.aspx in the Documents module in Microsoft SharePoint before 2010 uses URLs with the same hostname and port number for a web site's primary files and individual users' uploaded files (aka attachments), which allows remote authenticated users to leverage same-origin relationships and conduct cross-site scripting (XSS) attacks by uploading TXT files, a related issue to CVE-2008-5026. NOTE: the vendor disputes the significance of this issue, because cross-domain isolation can be implemented when needed.

Test Case Impact: Vulnerability Impact: Risk: **Low**

References:

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/509683/100/0/threaded

MISC: http://www.hacktics.com/content/advisories/AdvMS20100222.html

CVE Reference: CVE-2010-0716

- **CVE-2010-0107 Symantec CVSS 2.0 Score = 9.3**

Buffer overflow in an ActiveX control (SYMLTCOM.dll) in Symantec N360 1.0 and 2.0; Norton Internet Security, AntiVirus, SystemWorks, and Confidential 2006 through 2008; and Symantec Client Security 3.0.x before 3.1 MR9, and 3.1.x before MR9; allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unknown vectors. NOTE: this is only a vulnerability if the attacker can "masquerade as an authorized site."

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

References:

XF: http://xforce.iss.net/xforce/xfdb/56357

VUPEN: http://www.vupen.com/english/advisories/2010/0411

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

SECTRACK: http://www.securitytracker.com/id?1023631

SECTRACK: http://www.securitytracker.com/id?1023630

SECTRACK: http://www.securitytracker.com/id?1023629

SECTRACK: http://www.securitytracker.com/id?1023628

BID: http://www.securityfocus.com/bid/38217

SECUNIA: http://secunia.com/advisories/38654

OSVDB: http://osvdb.org/62412

CVE Reference: CVE-2010-0107

- **CVE-2010-0715 IBM CVSS 2.0 Score = 6.8**

Open redirect vulnerability in login.jsp in IBM WebSphere Portal, IBM Lotus Web Content Management (WCM), and IBM Lotus Workplace Web Content Management 5.1.0.0 through 5.1.0.5, 6.0.0.0 through 6.0.0.4, 6.0.1.0 through 6.0.1.7, 6.1.0.0 through 6.1.0.3, and 6.1.5.0; and IBM Lotus Quickr services 8.0, 8.0.0.2, 8.1, 8.1.1, and 8.1.1.1 for WebSphere Portal; allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via the query string.

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

References:

MISC: http://www-01.ibm.com/support/docview.wss?uid=swg21421469

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/509744/100/0/threaded

MISC: http://www.hacktics.com/content/advisories/AdvIBM20100224.html

CVE Reference: CVE-2010-0715

- **CVE-2010-0148 Cisco CVSS 2.0 Score = 7.8**

Unspecified vulnerability in Cisco Security Agent 5.2 before 5.2.0.285, when running on Linux, allows remote attackers to cause a denial of service (kernel panic) via "a series of TCP packets."

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

References:

SECUNIA: http://secunia.com/advisories/38619

XF: http://xforce.iss.net/xforce/xfdb/56347

VUPEN: http://www.vupen.com/english/advisories/2010/0416

SECTRACK: http://www.securitytracker.com/id?1023607

BID: http://www.securityfocus.com/bid/38273

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b1910d.shtml

OSVDB: http://osvdb.org/62445

CVE Reference: CVE-2010-0148

- **CVE-2010-0146 Cisco CVSS 2.0 Score = 6.8**

Directory traversal vulnerability in the Management Center for Cisco Security Agents 6.0 allows remote authenticated users to read arbitrary files via unspecified vectors.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/56345

VUPEN: http://www.vupen.com/english/advisories/2010/0416

SECTRACK: http://www.securitytracker.com/id?1023606

BID: http://www.securityfocus.com/bid/38271

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b1910d.shtml

SECUNIA: http://secunia.com/advisories/38619

OSVDB: http://osvdb.org/62443

CVE Reference: CVE-2010-0146

- **CVE-2009-1571 Mozilla CVSS 2.0 Score = 10.0**

Use-after-free vulnerability in the HTML parser in Mozilla Firefox 3.0.x before 3.0.18 and 3.5.x before 3.5.8, Thunderbird before 3.0.2, and SeaMonkey before 2.0.3 allows remote attackers to execute arbitrary code via unspecified method calls that attempt to access freed objects in low-memory situations.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=526500

XF: http://xforce.iss.net/xforce/xfdb/56361

VUPEN: http://www.vupen.com/english/advisories/2010/0405

UBUNTU: http://www.ubuntu.com/usn/USN-896-1

UBUNTU: http://www.ubuntu.com/usn/USN-895-1

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/509585/100/0/threaded

REDHAT: http://www.redhat.com/support/errata/RHSA-2010-0113.html

REDHAT: http://www.redhat.com/support/errata/RHSA-2010-0112.html

CONFIRM: http://www.mozilla.org/security/announce/2010/mfsa2010-03.html

MANDRIVA: http://www.mandriva.com/security/advisories?name=MDVSA-2010:042

DEBIAN: http://www.debian.org/security/2010/dsa-1999

MISC: http://secunia.com/secunia_research/2009-45/

SECUNIA: http://secunia.com/advisories/37242

FEDORA: http://lists.fedoraproject.org/pipermail/package-announce/2010-February/035426.html

FEDORA: http://lists.fedoraproject.org/pipermail/package-announce/2010-February/035367.html

FEDORA: http://lists.fedoraproject.org/pipermail/package-announce/2010-February/035346.html

CVE Reference: CVE-2009-1571

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