ScoutNews
The weekly Security update from the makers of SecureScout
July 30, 2010

2010 Issue #31

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

This Week in Review

Cybercrime is costly. SSL vulnerable via MITM. 1M fine for HIPAA violation. Hackers gain access due to configuration errors.

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

- **Cybercrime costs businesses $3.8 million per year**

Web attacks, malware and insider threats can cost organizations millions of dollars in losses each year, according to a Ponemon Institute study released Monday. The survey of 45 U.S. organizations, sponsored by security and compliance solutions provider ArcSight, found that cybercrime costs organizations $3.8 million per year on average. IT security practitioners at each of the participating entities were interviewed as part of the study, which found that the cost of cybercrime ranged from $1 million to $52 million per year per company.

Larry Ponemon, chairman and founder of the Ponemon Institute, told SCMagazineUS.com on Monday that some of the organizations studied were surprised at the total economic impact of digital offenses.

"Basically, the No. 1 takeaway is that cybercrime is very costly," Ponemon said. SC Magazine

Full Story :
http://www.scmagazineus.com/cybercrime-costs-businesses-38-million-per-year/article/175466/?utm_source=feedbu

- **Black Hat 2010: Even with SSL/TLS, browsers still are susceptible to attack**

Two researchers at the Black Hat conference in Las Vegas on Thursday exposed 24 ways hackers can hijack seemingly secure browser sessions.

Robert Hansen and Josh Sokol demonstrated methods attackers can use to take over users' accounts or assume control of a website without the need for any exploits, due to the way browsers implement "HTTPS." HTTPS, a combination of the Hypertext Transfer Protocol with the SSL/TLS Protocol, allows a website owner to encrypt a session using a digital certificate.

For any of the two dozen attacks to work, however, a criminal would have to have assumed control of a user's computer via a man-in-the-middle (MITM) exploit, by which an attacker intercepts communications between two systems. SC Magazine

Full Story :
http://www.scmagazineus.com/black-hat-2010-even-with-ssltls-browsers-still-are-susceptible-to-attack/article/17591

- **Rite Aid to pay $1 million fine for HIPAA violation**

Following federal charges that it violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule by improperly disposing of prescription information, pharmacy chain Rite Aid Corp. and its 40 affiliated entities (RAC) have agreed to pay a $1 million fine.

The fine was levied by the Office for Civil Rights (OCR), which enforces the HIPAA privacy and security rules from within the Department of Health and Human Services. OCR also required that RAC take corrective action to improve policies and procedures to safeguard the privacy of its customers when disposing of identifying information on pill bottle labels and other health information.

In addition to the OCR charge, the Federal Trade Commission also demanded the company undergo frequent security audits. SC Magazine

Full Story :
http://www.scmagazineus.com/rite-aid-to-pay-1-million-fine-for-hipaa-violation/article/175729/?utm_source=feedburn

- **Verizon: Data breaches often caused by configuration errors**

IDG News Service - Hackers appear to be increasingly counting on configuration problems and programming errors rather than software vulnerabilities in order to steal information from computer systems, according to a new study from Verizon.

Verizon issues an annual report on data breaches, but this year had access to statistics related to investigations done by the U.S. Secret Service, which the company said broadened the scope of its analysis. For 2009, that covered 141 cases involving 143 million records.

Verizon said it found that a surprising and "even shocking" trend is continuing: There are fewer attacks that focus on a software vulnerabilities than attacks that focus on configuration weaknesses or sloppy coding of an application. Computerworld

Full Story :
http://www.computerworld.com/s/article/9179848/Verizon_Data_breaches_often_caused_by_configuration_errors?so

New Vulnerabilities Tested in SecureScout

- **13759 Oracle Database Server - Listener component unspecified Vulnerability (jul-2010/CVE-2010-0911)**

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

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2010.html
* VUPEN: VUPEN/ADV-2010-1814
http://www.vupen.com/english/advisories/2010/1814
* BID: 41624
http://www.securityfocus.com/bid/41624
* SECTRACK: 1024192
http://securitytracker.com/alerts/2010/Jul/1024192.html

CVE Reference:

CVE-2010-0911 (cve.mitre.org, nvd.nist.gov)

• 13760 Oracle Database Server - Net Foundation Layer component unspecified Vulnerability (jul-2010/CVE-2010-0903)

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

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2010.html
* VUPEN: VUPEN/ADV-2010-1814
http://www.vupen.com/english/advisories/2010/1814
* BID: 41639
http://www.securityfocus.com/bid/41639
* SECTRACK: 1024192
http://securitytracker.com/alerts/2010/Jul/1024192.html

CVE Reference:

CVE-2010-0903 (cve.mitre.org, nvd.nist.gov)

• 13761 Oracle Database Server - Oracle OLAP component unspecified Vulnerability (jul-2010/CVE-2010-0902)

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

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

References:

* VUPEN: VUPEN/ADV-2010-1814
http://www.vupen.com/english/advisories/2010/1814
* BID: 41643
http://www.securityfocus.com/bid/41643
* SECTRACK: 1024192
http://securitytracker.com/alerts/2010/Jul/1024192.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2010.html

CVE Reference:

CVE-2010-0902 (cve.mitre.org, nvd.nist.gov)

• 13763 Oracle Database Server - Network Layer component unspecified Vulnerability (jul-2010/CVE-2010-0900)

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

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

References:

* VUPEN: VUPEN/ADV-2010-1814
http://www.vupen.com/english/advisories/2010/1814
* BID: 41632
http://www.securityfocus.com/bid/41632
* SECTRACK: 1024192
http://securitytracker.com/alerts/2010/Jul/1024192.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2010.html

CVE Reference:

CVE-2010-0900 (cve.mitre.org, nvd.nist.gov)

• 13764 Oracle Database Server -Export component unspecified Vulnerability (jul-2010/CVE-2010-0901)

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

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

References:

* VUPEN: VUPEN/ADV-2010-1814
http://www.vupen.com/english/advisories/2010/1814
* BID: 41635
http://www.securityfocus.com/bid/41635
* SECTRACK: 1024192
http://securitytracker.com/alerts/2010/Jul/1024192.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2010.html

CVE Reference:

CVE-2010-0901 (cve.mitre.org, nvd.nist.gov)

• 14594 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-2212) (Rmote File Checking)

Buffer overflow in Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via a PDF file containing Flash content with a crafted #1023 (3FFh) tag, a different vulnerability than CVE-2010-1295, CVE-2010-2202, CVE-2010-2207, CVE-2010-2209, CVE-2010-2210, and CVE-2010-2211.

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

References:

* SECTRACK: 1024159
http://securitytracker.com/alerts/2010/Jun/1024159.html
* VUPEN: VUPEN/ADV-2010-1636
http://www.vupen.com/english/advisories/2010/1636
* BID: 41245
http://www.securityfocus.com/bid/41245
* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb10-15.html

CVE Reference:

CVE-2010-2212 (cve.mitre.org, nvd.nist.gov)

• 18859 Wireshark DOCSIS dissector denial of service Vulnerability (Remote File Checking)

The DOCSIS dissector in Wireshark 0.9.6 through 1.0.12 and 1.2.0 through 1.2.7 allows user-assisted remote attackers to cause a denial of service (application crash) via a malformed packet trace file.

The vulnerability is reported in versions 0.9.6 up to and including 1.0.12, 1.2.0 up to and including 1.2.7.

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

References:

* MLIST: [oss-security] 20100507 Re: CVE Assignment (wireshark)
http://www.openwall.com/lists/oss-security/2010/05/07/7
* CONFIRM:
http://www.wireshark.org/security/wnpa-sec-2010-03.html
* CONFIRM:
http://www.wireshark.org/security/wnpa-sec-2010-04.html
* CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=4644
* CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=4646
* MANDRIVA: MDVSA-2010:099
http://www.mandriva.com/security/advisories?name=MDVSA-2010:099
* BID: 39950
http://www.securityfocus.com/bid/39950
* OSVDB: 64363
http://www.osvdb.org/64363
* SECUNIA: 39661
http://secunia.com/advisories/39661
* VUPEN: ADV-2010-1081
http://www.vupen.com/english/advisories/2010/1081
* XF: wireshark-docsis-dos(58362)

http://xforce.iss.net/xforce/xfdb/58362

CVE Reference:

CVE-2010-1455 (cve.mitre.org, nvd.nist.gov)

• 18860 Wireshark SMB dissector denial of service Vulnerability (CVE-2010-2283) (Remote File Checking)

The SMB dissector in Wireshark 0.99.6 through 1.0.13, and 1.2.0 through 1.2.8 allows remote attackers to cause a denial of service (NULL pointer dereference) via unknown vectors.

The vulnerability is reported in versions 0.99.6 up to and including 1.0.13, 1.2.0 up to and including 1.2.8.

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

References:

* MLIST: [oss-security] 20100610 CVE request for new wireshark vulnerabilities
http://www.openwall.com/lists/oss-security/2010/06/11/1
* CONFIRM:
http://www.wireshark.org/security/wnpa-sec-2010-05.html
* CONFIRM:
http://www.wireshark.org/security/wnpa-sec-2010-06.html
* MANDRIVA: MDVSA-2010:113
http://www.mandriva.com/security/advisories?name=MDVSA-2010:113
* BID: 40728
http://www.securityfocus.com/bid/40728
* SECUNIA: 40112
http://secunia.com/advisories/40112
* VUPEN: ADV-2010-1418
http://www.vupen.com/english/advisories/2010/1418

CVE Reference:

CVE-2010-2283 (cve.mitre.org, nvd.nist.gov)

• 18861 Wireshark ASN.1 BER buffer overflow Vulnerability (Remote File Checking)

Buffer overflow in the ASN.1 BER dissector in Wireshark 0.10.13 through 1.0.13 and 1.2.0 through 1.2.8 has unknown impact and remote attack vectors.

The vulnerability is reported in versions 0.10.13 up to and including 1.0.13, 1.2.0 up to and including 1.2.8.

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

References:

* MLIST: [oss-security] 20100610 CVE request for new wireshark vulnerabilities
http://www.openwall.com/lists/oss-security/2010/06/11/1
* CONFIRM:
http://www.wireshark.org/security/wnpa-sec-2010-05.html
* CONFIRM:
http://www.wireshark.org/security/wnpa-sec-2010-06.html
* MANDRIVA: MDVSA-2010:113
http://www.mandriva.com/security/advisories?name=MDVSA-2010:113
* BID: 40728
http://www.securityfocus.com/bid/40728
* SECUNIA: 40112
http://secunia.com/advisories/40112
* VUPEN: ADV-2010-1418
http://www.vupen.com/english/advisories/2010/1418

CVE Reference:

CVE-2010-2284 (cve.mitre.org, nvd.nist.gov)

• 18862 Wireshark SMB PIPE denial of service Vulnerability (Remote File Checking)

The SMB PIPE dissector in Wireshark 0.8.20 through 1.0.13 and 1.2.0 through 1.2.8 allows remote attackers to cause a denial of service (NULL pointer dereference) via unknown vectors.

The vulnerability is reported in versions 0.8.20 up to and including 1.0.13, 1.2.0 up to and including 1.2.8.

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

References:

* MLIST: [oss-security] 20100610 CVE request for new wireshark vulnerabilities
http://www.openwall.com/lists/oss-security/2010/06/11/1
* CONFIRM:
http://www.wireshark.org/security/wnpa-sec-2010-05.html
* CONFIRM:
http://www.wireshark.org/security/wnpa-sec-2010-06.html
* MANDRIVA: MDVSA-2010:113
http://www.mandriva.com/security/advisories?name=MDVSA-2010:113
* BID: 40728
http://www.securityfocus.com/bid/40728
* SECUNIA: 40112
http://secunia.com/advisories/40112
* VUPEN: ADV-2010-1418
http://www.vupen.com/english/advisories/2010/1418

CVE Reference:

CVE-2010-2285 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-1452 Apache CVSS 2.0 Score = 5.0

The (1) mod_cache and (2) mod_dav modules in the Apache HTTP Server 2.2.x before 2.2.16 allow remote attackers to cause a denial of service (process crash) via a request that lacks a path.

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

References:

MLIST: http://marc.info/?l=apache-announce&m=128009718610929&w=2

CONFIRM: https://issues.apache.org/bugzilla/show_bug.cgi?id=49246

CONFIRM: http://httpd.apache.org/security/vulnerabilities_22.html

CVE Reference: CVE-2010-1452

• CVE-2010-2703 HP CVSS 2.0 Score = 10.0

Stack-based buffer overflow in the execvp_nc function in the ov.dll module in HP OpenView Network Node Manager (OV NNM) 7.51 and 7.53, when running on Windows, allows remote attackers to execute arbitrary code via a long HTTP request to webappmon.exe.

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

References:

HP: http://marc.info/?l=bugtraq&m=127973001009749&w=2

HP: http://marc.info/?l=bugtraq&m=127973001009749&w=2

VUPEN: http://www.vupen.com/english/advisories/2010/1866

SECTRACK: http://www.securitytracker.com/id?1024238

SECTRACK: http://www.securitytracker.com/id?1024224

BID: http://www.securityfocus.com/bid/41829

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/512552/100/0/threaded

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/512544/100/0/threaded

VIM: http://www.attrition.org/pipermail/vim/2010-July/002374.html

SECUNIA: http://secunia.com/advisories/40686

OSVDB: http://osvdb.org/66514

CVE Reference: CVE-2010-2703

- **CVE-2010-2704 HP CVSS 2.0 Score = 10.0**

Buffer overflow in HP OpenView Network Node Manager (OV NNM) 7.51 and 7.53 allows remote attackers to execute arbitrary code via a long HTTP request to nnmrptconfig.exe.

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

References:

HP: http://marc.info/?l=bugtraq&m=127972286628707&w=2

HP: http://marc.info/?l=bugtraq&m=127972286628707&w=2

VUPEN: http://www.vupen.com/english/advisories/2010/1866

BID: http://www.securityfocus.com/bid/41839

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/512543/100/0/threaded

VIM: http://www.attrition.org/pipermail/vim/2010-July/002374.html

SECUNIA: http://secunia.com/advisories/40697

HP: http://marc.info/?l=bugtraq&m=127974889107645&w=2

CVE Reference: CVE-2010-2704

- **CVE-2010-2896 IBM CVSS 2.0 Score = 4.3**

IBM FileNet Content Manager (CM) 4.0.0, 4.0.1, 4.5.0, and 4.5.1 before FP4 does not properly manage the InheritParentPermissions setting during an upgrade from 3.x, which might allow attackers to bypass intended folder permissions via unspecified vectors.

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

References:

VUPEN: http://www.vupen.com/english/advisories/2010/1847

CONFIRM: http://www-01.ibm.com/support/docview.wss?uid=swg21441225

SECUNIA: http://secunia.com/advisories/40614

CVE Reference: CVE-2010-2896

- **CVE-2010-1577 Cisco CVSS 2.0 Score = 7.8**

Directory traversal vulnerability in Cisco Internet Streamer, as used in Cisco Content Delivery System (CDS) 2.2.x, 2.3.x, 2.4.x, and 2.5.x before 2.5.7 allows remote attackers to read arbitrary files via a crafted URL.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b3bd1c.shtml

XF: http://xforce.iss.net/xforce/xfdb/60567

VUPEN: http://www.vupen.com/english/advisories/2010/1881

SECTRACK: http://www.securitytracker.com/id?1024234

SECUNIA: http://secunia.com/advisories/40701

OSVDB: http://osvdb.org/66508

CVE Reference: CVE-2010-1577

- **CVE-2010-2904 Sap CVSS 2.0 Score = 4.3**

Multiple cross-site scripting (XSS) vulnerabilities in the System Landscape Directory (SLD) component 6.4 through 7.02 in SAP NetWeaver allow remote attackers to inject arbitrary web script or HTML via the (1) action parameter to testsdic and the (2) helpstring parameter to paramhelp.jsp.

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

References:

MISC: https://service.sap.com/sap/support/notes/1416047

XF: http://xforce.iss.net/xforce/xfdb/60668

VUPEN: http://www.vupen.com/english/advisories/2010/1935

OSVDB: http://www.osvdb.org/66640

OSVDB: http://www.osvdb.org/66639

SECUNIA: http://secunia.com/advisories/40712

MISC: http://packetstormsecurity.org/1007-advisories/DSECRG-09-068.txt

MISC: http://dsecrg.com/pages/vul/show.php?id=168

CVE Reference: CVE-2010-2904

- **CVE-2010-2897 Google CVSS 2.0 Score = 10.0**

Google Chrome before 5.0.375.125 does not properly mitigate an unspecified flaw in the Windows kernel, which has unknown impact and attack vectors.

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

References:

SECUNIA: http://secunia.com/advisories/40743

CONFIRM: http://googlechromereleases.blogspot.com/2010/07/stable-channel-update_26.html

CONFIRM: http://code.google.com/p/chromium/issues/detail?id=48283

CVE Reference: CVE-2010-2897

- **CVE-2010-2898 Google CVSS 2.0 Score = 10.0**

Google Chrome before 5.0.375.125 does not properly mitigate an unspecified flaw in the GNU C Library, which has unknown impact and attack vectors.

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

References:

SECUNIA: http://secunia.com/advisories/40743

CONFIRM: http://googlechromereleases.blogspot.com/2010/07/stable-channel-update_26.html

CONFIRM: http://code.google.com/p/chromium/issues/detail?id=48733

CVE Reference: CVE-2010-2898

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