ScoutNews
The weekly Security update from the makers of SecureScout
November 19, 2010

2010 Issue #46

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

Stuxnet targets infrastructure. China accused of rerouting internet traffic. Credit Card thief charged. Our George Orwellian future.

netVigilance Carbon Neutral in 2010
Through careful resource management and optimal use of energy saving technology, combined with a Carbon offset payment spent on alternative energy and reforestation projects, netVigilance managed to become Carbon Neutral in 2010.
Jesper Jurcenoks from netVigilance explains: "Making the internet safer and making the planet healthier goes hand in hand with netVigilance's core vision of Quality, Efficiency and Integrity".

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

- **Symantec to Congress: Stuxnet is 'wake-up call'**

Dean Turner, director of the Global Intelligence Network at Symantec Security Response

(Credit: Symantec)

The Stuxnet worm is a "wake-up call" because of its complexity and its aim at critical infrastructure systems, a Symantec director told a U.S. congressional committee today. Cnet Security

Full Story :
http://news.cnet.com/8301-27080_3-20023124-245.html?part=rss&subj=news&tag=2547-1_3-0-20

- **Update: Report sounds alarm on China's rerouting of U.S. Internet traffic**

Computerworld - A report submitted to Congress on Wednesday by the U.S.-China Economic and Security Review Commission expressed concerns over what the commission claims is China's growing ability to control and manipulate Internet traffic.

The report points to two specific incidents earlier this year where actions taken inside China had a direct impact on Internet traffic in the U.S. and other regions of the world.

In one of the incidents, traffic to and from about 15% of all Internet destinations was routed through servers belonging to China Telecom, a state-owned telecommunications company. Computerworld

Full Story :
http://www.computerworld.com/s/article/9197019/Update_Report_sounds_alarm_on_China_s_rerouting_of_U.S._Inte

- **Malaysian charged with hacking Federal Reserve, others**

IDG News Service - A Malaysian man has been charged with hacking into major U.S. corporations, including the U.S. Federal Reserve Bank of Cleveland and FedComp, a company that processes financial transactions for credit unions.

Lin Mun Poo, 32, was arrested on Oct. 21, just hours after flying into New York and selling $1,000 worth of stolen credit card numbers at a Brooklyn diner, prosecutors said. After inspecting his laptop, U.S. Secret Service investigators found more than "400,000 stolen credit and debit card account numbers allegedly obtained by hacking into various computer systems of other financial institutions," the Secret Service said in a news release. Computerworld

Full Story :
http://www.computerworld.com/s/article/9197220/Malaysian_charged_with_hacking_Federal_Reserve_others?source

- **My own private memory hole**

Editors' note: This is a guest column. See Larry Downes' bio below.

In "1984," George Orwell's classic dystopian novel, protagonist Winston Smith is a low-level bureaucrat in the Ministry of Truth. His job: to "rectify" old newspaper articles in which Big Brother's predictions or promises turned out to be false. Once the articles are rewritten, the original text--and the truth they represent--is dropped down a pneumatic tube known as a memory hole, "to be devoured by the flames."

The European Commission has recently proposed a real-life version of this fictional device, though this time with a twist. Twenty-five years after the events in Orwell's allegory took place, the Commission has announced plans to regulate what it calls an individual's "right to be forgotten." The new memory hole would be under the control not of Big Brother but of individuals--of all the Winston Smiths of the world. Cnet Security

Full Story :
http://news.cnet.com/8301-13578_3-20022977-38.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

- **13771 Oracle Database Server - EM Console component unspecified Vulnerability (oct-2010/CVE-2010-2390)**

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

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

References:

* CONFIRM:
http://www.oracle.com/technetwork/topics/security/cpuoct2010-175626.html
* CERT: TA10-287A
http://www.us-cert.gov/cas/techalerts/TA10-287A.html
* BID: 43945
http://www.securityfocus.com/bid/43945
* SECTRACK: 1024560
http://securitytracker.com/alerts/2010/Oct/1024560.html
* VUPEN: VUPEN/ADV-2010-2642
http://www.vupen.com/english/advisories/2010/2642

CVE Reference:

CVE-2010-2390 (cve.mitre.org, nvd.nist.gov)

• 13772 Oracle Database Server - Java Virtual Machine component unspecified Vulnerability (oct-2010/CVE-2010-2419)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Java Virtual Machine" component.

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

References:

* BID: 43935
http://www.securityfocus.com/bid/43935
* SECTRACK: 1024560
http://securitytracker.com/alerts/2010/Oct/1024560.html
* VUPEN: VUPEN/ADV-2010-2642
http://www.vupen.com/english/advisories/2010/2642
* CONFIRM:
http://www.oracle.com/technetwork/topics/security/cpuoct2010-175626.html
* CERT: TA10-287A
http://www.us-cert.gov/cas/techalerts/TA10-287A.html

CVE Reference:

CVE-2010-2419 (cve.mitre.org, nvd.nist.gov)

• 13773 Oracle Database Server - Change Data Capture component unspecified Vulnerability (oct-2010/CVE-2010-1321)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Change Data Capture" component.

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

References:

* BID: 40235
http://www.securityfocus.com/bid/40235
* SECTRACK: 1024560
http://securitytracker.com/alerts/2010/Oct/1024560.html
* VUPEN: VUPEN/ADV-2010-2642
http://www.vupen.com/english/advisories/2010/2642
* BUGTRAQ: 20100518 MITKRB5-SA-2010-005 [CVE-2010-1321] GSS-API lib null pointer deref
http://www.securityfocus.com/archive/1/archive/1/511331/100/0/threaded
* CONFIRM:
http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2010-005.txt
* CONFIRM:
http://support.avaya.com/css/P8/documents/100114315
* CONFIRM:
http://www.oracle.com/technetwork/topics/security/javacpuoct2010-176258.html
* DEBIAN: DSA-2052
http://www.debian.org/security/2010/dsa-2052
* FEDORA: FEDORA-2010-8749
http://lists.fedoraproject.org/pipermail/package-announce/2010-May/041615.html
* FEDORA: FEDORA-2010-8796
http://lists.fedoraproject.org/pipermail/package-announce/2010-May/041645.html
* FEDORA: FEDORA-2010-8805
http://lists.fedoraproject.org/pipermail/package-announce/2010-May/041654.html
* HP: HPSBUX02544
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02257427
* MANDRIVA: MDVSA-2010:100
http://www.mandriva.com/security/advisories?name=MDVSA-2010:100
* REDHAT: RHSA-2010:0423
http://www.redhat.com/support/errata/RHSA-2010-0423.html
* REDHAT: RHSA-2010:0770
http://www.redhat.com/support/errata/RHSA-2010-0770.html
* REDHAT: RHSA-2010:0807
http://www.redhat.com/support/errata/RHSA-2010-0807.html
* SUSE: SUSE-SR:2010:013
http://lists.opensuse.org/opensuse-security-announce/2010-06/msg00001.html
* SUSE: SUSE-SR:2010:014
http://lists.opensuse.org/opensuse-security-announce/2010-08/msg00001.html
* UBUNTU: USN-940-1

http://www.ubuntu.com/usn/USN-940-1
* UBUNTU: USN-940-2
http://www.ubuntu.com/usn/USN-940-2
* CERT: TA10-287A
http://www.us-cert.gov/cas/techalerts/TA10-287A.html
* OSVDB: 64744
http://osvdb.org/64744
* OVAL: oval:org.mitre.oval:def:11604
http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11604
* SECUNIA: 39762
http://secunia.com/advisories/39762
* SECUNIA: 39818
http://secunia.com/advisories/39818
* SECUNIA: 39784
http://secunia.com/advisories/39784
* SECUNIA: 39799
http://secunia.com/advisories/39799
* SECUNIA: 39849
http://secunia.com/advisories/39849
* SECUNIA: 40346
http://secunia.com/advisories/40346
* SECUNIA: 40685
http://secunia.com/advisories/40685
* SECUNIA: 41967
http://secunia.com/advisories/41967
* VUPEN: ADV-2010-1177
http://www.vupen.com/english/advisories/2010/1177
* VUPEN: ADV-2010-1193
http://www.vupen.com/english/advisories/2010/1193
* VUPEN: ADV-2010-1196
http://www.vupen.com/english/advisories/2010/1196
* VUPEN: ADV-2010-1192
http://www.vupen.com/english/advisories/2010/1192
* VUPEN: ADV-2010-1222
http://www.vupen.com/english/advisories/2010/1222
* VUPEN: ADV-2010-1574
http://www.vupen.com/english/advisories/2010/1574
* VUPEN: ADV-2010-1882
http://www.vupen.com/english/advisories/2010/1882

CVE Reference:

CVE-2010-1321 (cve.mitre.org, nvd.nist.gov)

• 13774 Oracle Database Server - OLAP component unspecified Vulnerability (oct-2010/CVE-2010-2412)

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

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

References:

* BID: 43940
http://www.securityfocus.com/bid/43940
* SECTRACK: 1024560
http://securitytracker.com/alerts/2010/Oct/1024560.html
* VUPEN: VUPEN/ADV-2010-2642
http://www.vupen.com/english/advisories/2010/2642
* CONFIRM:
http://www.oracle.com/technetwork/topics/security/cpuoct2010-175626.html
* CERT: TA10-287A
http://www.us-cert.gov/cas/techalerts/TA10-287A.html

CVE Reference:

CVE-2010-2412 (cve.mitre.org, nvd.nist.gov)

• 13775 Oracle Database Server - Change Data Capture component unspecified Vulnerability (oct-2010/CVE-2010-2415)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Change Data Capture" component.

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

References:

* BID: 43956
http://www.securityfocus.com/bid/43956
* SECTRACK: 1024560
http://securitytracker.com/alerts/2010/Oct/1024560.html
* VUPEN: VUPEN/ADV-2010-2642
http://www.vupen.com/english/advisories/2010/2642
* CONFIRM:
http://www.oracle.com/technetwork/topics/security/cpuoct2010-175626.html
* CERT: TA10-287A
http://www.us-cert.gov/cas/techalerts/TA10-287A.html

CVE Reference:

CVE-2010-2415 (cve.mitre.org, nvd.nist.gov)

• 13776 Oracle Database Server - Job Queue component unspecified Vulnerability (oct-2010/CVE-2010-2411)

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

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

References:

* BID: 43958
http://www.securityfocus.com/bid/43958
* SECTRACK: 1024560
http://securitytracker.com/alerts/2010/Oct/1024560.html
* VUPEN: VUPEN/ADV-2010-2642
http://www.vupen.com/english/advisories/2010/2642
* CONFIRM:
http://www.oracle.com/technetwork/topics/security/cpuoct2010-175626.html
* CERT: TA10-287A
http://www.us-cert.gov/cas/techalerts/TA10-287A.html

CVE Reference:

CVE-2010-2411 (cve.mitre.org, nvd.nist.gov)

• 13777 Oracle Database Server - XDK component unspecified Vulnerability (oct-2010/CVE-2010-2407)

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

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

References:

* BID: 43970
http://www.securityfocus.com/bid/43970
* SECTRACK: 1024560
http://securitytracker.com/alerts/2010/Oct/1024560.html
* VUPEN: VUPEN/ADV-2010-2642
http://www.vupen.com/english/advisories/2010/2642
* CONFIRM:
http://www.oracle.com/technetwork/topics/security/cpuoct2010-175626.html
* CERT: TA10-287A
http://www.us-cert.gov/cas/techalerts/TA10-287A.html

CVE Reference:

CVE-2010-2407 (cve.mitre.org, nvd.nist.gov)

• 13778 Oracle Database Server - Core RDBMS component unspecified Vulnerability (oct-2010/CVE-2010-2391)

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

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

References:

* BID: 43961
http://www.securityfocus.com/bid/43961
* SECTRACK: 1024560
http://securitytracker.com/alerts/2010/Oct/1024560.html
* VUPEN: VUPEN/ADV-2010-2642
http://www.vupen.com/english/advisories/2010/2642
* CONFIRM:
http://www.oracle.com/technetwork/topics/security/cpuoct2010-175626.html
* CERT: TA10-287A
http://www.us-cert.gov/cas/techalerts/TA10-287A.html

CVE Reference:

CVE-2010-2391 (cve.mitre.org, nvd.nist.gov)

- **13779 Oracle Database Server - Perl component unspecified Vulnerability (oct-2010/CVE-2010-2389)**

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

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

References:

* BID: 43964
http://www.securityfocus.com/bid/43964
* SECTRACK: 1024560
http://securitytracker.com/alerts/2010/Oct/1024560.html
* VUPEN: VUPEN/ADV-2010-2642
http://www.vupen.com/english/advisories/2010/2642
* CONFIRM:
http://www.oracle.com/technetwork/topics/security/cpuoct2010-175626.html
* CERT: TA10-287A
http://www.us-cert.gov/cas/techalerts/TA10-287A.html

CVE Reference:

CVE-2010-2389 (cve.mitre.org, nvd.nist.gov)

- **19000 Embedded OpenType Font Integer Overflow Vulnerability (MS10-076/982132) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Windows Embedded OpenType (EOT) font technology parses certain tables in specially crafted embedded fonts. 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:

* VUPEN: VUPEN/ADV-2010-2623
http://www.vupen.com/english/advisories/2010/2623
* BID: 43775
http://www.securityfocus.com/bid/43775
* SECTRACK: 1024544
http://securitytracker.com/alerts/2010/Oct/1024544.html
* MS: MS10-076
http://www.microsoft.com/technet/security/Bulletin/MS10-076.mspx

CVE Reference:

CVE-2010-1883 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- **CVE-2010-4107 HP CVSS 2.0 Score = 7.8**

The default configuration of the PJL Access value in the File System External Access settings on HP LaserJet MFP printers, Color LaserJet MFP printers, and LaserJet 4100, 4200, 4300, 5100, 8150, and 9000 printers enables PJL

commands that use the device's filesystem, which allows remote attackers to read arbitrary files via a command inside a print job, as demonstrated by a directory traversal attack.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/63261

VUPEN: http://www.vupen.com/english/advisories/2010/2987

HP: http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02004333

HP: http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02004333

SECTRACK: http://securitytracker.com/id?1024741

SECUNIA: http://secunia.com/advisories/42238

CVE Reference: CVE-2010-4107

- **CVE-2010-0113 Symantec CVSS 2.0 Score = 6.0**

The Symantec Norton Mobile Security application 1.0 Beta for Android records setup details, possibly including wipe/lock credentials, in the device logs, which allows user-assisted remote attackers to obtain potentially sensitive information by leveraging the ability of a separate crafted application to read these logs.

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

References:

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

BID: http://www.securityfocus.com/bid/44767

CVE Reference: CVE-2010-0113

- **CVE-2010-4274 IBM CVSS 2.0 Score = 4.4**

reset_diragent_keys in the Common agent in IBM Systems Director 6.2.0 has 754 permissions, which allows local users to gain privileges by leveraging system group membership.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/63238

VUPEN: http://www.vupen.com/english/advisories/2010/2978

BID: http://www.securityfocus.com/bid/44839

AIXAPAR: http://www-01.ibm.com/support/docview.wss?uid=isg1IC71821

SECTRACK: http://securitytracker.com/id?1024736

SECUNIA: http://secunia.com/advisories/42239

CVE Reference: CVE-2010-4274

- **CVE-2010-2638 IBM CVSS 2.0 Score = 4.0**

Unspecified vulnerability in IBM WebSphere MQ 7.0 before 7.0.1.5 allows remote authenticated users to cause a denial of service (disk consumption) via vectors that trigger an FDC with an RM680004 Probe Id value.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/63147

CVE Reference: CVE-2010-2638

- **CVE-2010-1841 Apple CVSS 2.0 Score = 9.3**

Disk Images in Apple Mac OS X 10.5.8 and 10.6.x before 10.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted UDIF image.

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

References:

CONFIRM: http://support.apple.com/kb/HT4435

APPLE: http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html

CVE Reference: CVE-2010-1841

- **CVE-2010-1842 Apple CVSS 2.0 Score = 9.3**

Buffer overflow in AppKit in Apple Mac OS X 10.6.x before 10.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a bidirectional text string with ellipsis truncation.

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

References:

CONFIRM: http://support.apple.com/kb/HT4435

APPLE: http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html

CVE Reference: CVE-2010-1842

- **CVE-2010-1843 Apple CVSS 2.0 Score = 7.8**

Networking in Apple Mac OS X 10.6.2 through 10.6.4 allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted PIM packet.

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

References:

CONFIRM: http://support.apple.com/kb/HT4435

APPLE: http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html

CVE Reference: CVE-2010-1843

- **CVE-2010-1378 Apple CVSS 2.0 Score = 7.5**

OpenSSL in Apple Mac OS X 10.6.x before 10.6.5 does not properly perform arithmetic, which allows remote attackers to bypass X.509 certificate authentication via an arbitrary certificate issued by a legitimate Certification Authority.

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

References:

CONFIRM: http://support.apple.com/kb/HT4435

APPLE: http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html

CVE Reference: CVE-2010-1378

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