

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>

[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

Worries of governmental infrastructure attacks. Companies not really aware of cyber risks. Cost of data breach analysis. Ipad searches link to malicious sites.

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

• Report shows cyberattacks rampant; execs concerned

Critical infrastructure networks around the world are subject to repeated cyberattacks from foreign governments and other high-level adversaries that can be damaging and costly, according to a report McAfee released Thursday.

Attacks that lead to down time can cost more than \$6 million per day, and more than \$8 million at oil and gas companies, the report, "In the Crossfire--Critical Infrastructure in the Age of Cyberwar," found.

Meanwhile, respondents said they worry about attacks on critical infrastructure in their countries coming from the U.S.

and China more than any other potential aggressors. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-10441824-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• **Report: Companies unprepared for cybercrime**

Many organizations are focused on stopping random hackers and blocking pornography when they should be concerned with bigger threats from professional cybercriminals, according to a new cybersecurity report.

A new Deloitte report offers insight into organizations' perceptions on cyber incidents.

(Credit: Deloitte) Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-10440901-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• **Data breaches cost organizations \$204 per record in 2009**

Data breaches last year cost organizations \$204 per exposed record on average, which represents an almost two percent increase over 2008, according to the fifth annual "Cost of Data Breach" study released on Monday by the Ponemon Institute.

"I am surprised that the number keeps on going up," Larry Ponemon, chairman and founder of the Ponemon Institute, told SCMagazineUS.com on Friday. "Even though it's a small amount, it suggests to us that people still deeply care about data breaches."

The study, which examined the experiences of 45 U.S. companies that suffered breaches last year, also found that the number of data breaches that were caused by malicious attacks and botnets doubled from 12 percent in 2008 to 24 percent in 2009. In addition, data breaches caused by malicious attacks cost organizations 30 to 40 percent more on average than those caused by human negligence or by IT system glitches. SC Magazine

Full Story :

http://www.scmagazineus.com/data-breaches-cost-organizations-204-per-record-in-2009/article/162259/?utm_source

• **Web searches for iPad leading to malicious sites**

Security companies are warning consumers and Web site operators to be wary of iPad related search scams.

"This is just the kind of opportunity fraudsters like to exploit by poisoning search terms," said Symantec's Candid Wueest. Wueest also warned about "iPad-related spam and phishing attacks hitting consumers hard over the coming weeks."

In an interview, Don Debolt, CA's director of threat research, warned about "black hat search optimization"--a scam whereby hackers take advantage of security flaws in blogs and other sites that use PHP to imbed popular search terms like iPad to trick search engines into directing people to compromised legitimate sites that may have nothing to do with the subject matter at hand. If someone clicks on the link to a page on that infected site they are then redirected to a malicious site which can implant malware on their machine or tempt them to install a rogue security product. Cnet Security

Full Story :

http://news.cnet.com/8301-19518_3-10443931-238.html

New Vulnerabilities Tested in SecureScout

• **13748 Oracle Database Server - RDBMS component unspecified Vulnerability (jan-2010/CVE-2009-3410)**

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

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

References:

* BID: 37740

<http://www.securityfocus.com/bid/37740>

* SECTRACK: 1023436

<http://securitytracker.com/alerts/2010/Jan/1023436.html>

* VUPEN: VUPEN/ADV-2010-0102

<http://www.vupen.com/english/advisories/2010/0102>

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2010.html>

* CERT: TA10-012A

<http://www.us-cert.gov/cas/techalerts/TA10-012A.html>

CVE Reference:

CVE-2009-3410 (cve.mitre.org, nvd.nist.gov)

• **13749 Oracle Database Server - Oracle Spatial component unspecified Vulnerability (jan-2010/CVE-2009-3413)**

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

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

References:

* BID: 37740

<http://www.securityfocus.com/bid/37740>

* SECTRACK: 1023436

<http://securitytracker.com/alerts/2010/Jan/1023436.html>

* VUPEN: VUPEN/ADV-2010-0102

<http://www.vupen.com/english/advisories/2010/0102>

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2010.html>

* CERT: TA10-012A

<http://www.us-cert.gov/cas/techalerts/TA10-012A.html>

CVE Reference:

CVE-2009-3413 (cve.mitre.org, nvd.nist.gov)

• **13750 Oracle Database Server - Unzip component unspecified Vulnerability (jan-2010/CVE-2009-3412)**

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

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

References:

* BID: 37740

<http://www.securityfocus.com/bid/37740>

* SECTRACK: 1023436

<http://securitytracker.com/alerts/2010/Jan/1023436.html>

* VUPEN: VUPEN/ADV-2010-0102

<http://www.vupen.com/english/advisories/2010/0102>

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2010.html>

* CERT: TA10-012A

<http://www.us-cert.gov/cas/techalerts/TA10-012A.html>

CVE Reference:

CVE-2009-3412 (cve.mitre.org, nvd.nist.gov)

• **18688 Internet Explorer XSS Filter Script Handling Vulnerability (MS10-002/979352) (Remote File Checking)**

An XSS filter bypass vulnerability exists in the way that Internet Explorer 8 disables an HTML attribute in otherwise appropriately filtered HTTP response data. The vulnerability could allow initially disabled scripts to run in the wrong security context, leading to information disclosure.

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

References:

* MISC:

<http://hackademix.net/2009/11/21/ies-xss-filter-creates-xss-vulnerabilities/>

* MISC:

http://www.owasp.org/images/5/50/OWASP-Italy_Day_IV_Maone.pdf

* MISC:

http://www.theregister.co.uk/2009/11/20/internet_explorer_security_flaw/

* MS: MS10-002

<http://www.microsoft.com/technet/security/Bulletin/MS10-002.msp>

* BID: 37135

<http://www.securityfocus.com/bid/37135>

CVE Reference:

CVE-2009-4074 (cve.mitre.org, nvd.nist.gov)

• 18689 Internet Explorer URL Validation Vulnerability (MS10-002/979352) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer incorrectly validates input. An attacker could exploit the vulnerability by constructing a specially crafted URL. When a user clicks the URL, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. 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.

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

References:

* MS: MS10-002

<http://www.microsoft.com/technet/security/Bulletin/MS10-002.msp>

* XF: ie-url-code-execution(55773)

<http://xforce.iss.net/xforce/xfdb/55773>

* BID: 37884

<http://www.securityfocus.com/bid/37884>

* VUPEN: VUPEN/ADV-2010-0187

<http://www.vupen.com/english/advisories/2010/0187>

CVE Reference:

CVE-2010-0027 (cve.mitre.org, nvd.nist.gov)

• 18690 Internet Explorer Uninitialized Memory Corruption Vulnerability (CVE-2010-0244) (MS10-002/979352) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. 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.

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

References:

* BID: 37891

<http://www.securityfocus.com/bid/37891>

* VUPEN: VUPEN/ADV-2010-0187

<http://www.vupen.com/english/advisories/2010/0187>

* MS: MS10-002

<http://www.microsoft.com/technet/security/Bulletin/MS10-002.msp>

* XF: ie-deleted-obj-code-exec(55774)

<http://xforce.iss.net/xforce/xfdb/55774>

* SECTRACK: 1023493

<http://securitytracker.com/alerts/2010/Jan/1023493.html>

CVE Reference:

CVE-2010-0244 (cve.mitre.org, nvd.nist.gov)

• 18691 Internet Explorer Uninitialized Memory Corruption Vulnerability (CVE-2010-0245) (MS10-002/979352) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. 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.

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

References:

- * BID: 37891
<http://www.securityfocus.com/bid/37891>
- * VUPEN: VUPEN/ADV-2010-0187
<http://www.vupen.com/english/advisories/2010/0187>
- * SECTRACK: 1023493
<http://securitytracker.com/alerts/2010/Jan/1023493.html>
- * MS: MS10-002
<http://www.microsoft.com/technet/security/Bulletin/MS10-002.msp>
- * XF: ie-uninitialized-memory-code-exec(55775)
<http://xforce.iss.net/xforce/xfdb/55775>

CVE Reference:

CVE-2010-0245 (cve.mitre.org, nvd.nist.gov)

• 18692 Internet Explorer Uninitialized Memory Corruption Vulnerability (CVE-2010-0246) (MS10-002/979352) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. 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.

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

References:

- * BID: 37891
<http://www.securityfocus.com/bid/37891>
- * VUPEN: VUPEN/ADV-2010-0187
<http://www.vupen.com/english/advisories/2010/0187>
- * SECTRACK: 1023493
<http://securitytracker.com/alerts/2010/Jan/1023493.html>
- * MS: MS10-002
<http://www.microsoft.com/technet/security/Bulletin/MS10-002.msp>
- * XF: ie-deleted-object-code-exec(55776)
<http://xforce.iss.net/xforce/xfdb/55776>

CVE Reference:

CVE-2010-0246 (cve.mitre.org, nvd.nist.gov)

• 18693 Internet Explorer Uninitialized Memory Corruption Vulnerability (CVE-2010-0247) (MS10-002/979352) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. 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.

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

References:

- * BID: 37891
<http://www.securityfocus.com/bid/37891>
- * VUPEN: VUPEN/ADV-2010-0187
<http://www.vupen.com/english/advisories/2010/0187>
- * SECTRACK: 1023493
<http://securitytracker.com/alerts/2010/Jan/1023493.html>
- * MS: MS10-002
<http://www.microsoft.com/technet/security/Bulletin/MS10-002.msp>
- * XF: ie-uninitialized-obj-code-exec(55777)
<http://xforce.iss.net/xforce/xfdb/55777>

CVE Reference:

CVE-2010-0247 (cve.mitre.org, nvd.nist.gov)

• 18694 Internet Explorer HTML Object Memory Corruption Vulnerability (CVE-2010-0248) (MS10-002/979352) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. 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.

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

References:

* BID: 37891

<http://www.securityfocus.com/bid/37891>

* VUPEN: VUPEN/ADV-2010-0187

<http://www.vupen.com/english/advisories/2010/0187>

* SECTRAK: 1023493

<http://securitytracker.com/alerts/2010/Jan/1023493.html>

* MS: MS10-002

<http://www.microsoft.com/technet/security/Bulletin/MS10-002.msp>

* XF: ie-object-memory-code-exec(55778)

<http://xforce.iss.net/xforce/xfdb/55778>

CVE Reference:

CVE-2010-0248 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-2693 Apache CVSS 2.0 Score = 5.8

Directory traversal vulnerability in Apache Tomcat 5.5.0 through 5.5.28 and 6.0.0 through 6.0.20 allows remote attackers to create or overwrite arbitrary files via a .. (dot dot) in an entry in a WAR file, as demonstrated by a ../../bin/catalina.bat entry.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/0213>

CONFIRM: <http://tomcat.apache.org/security-6.html>

CONFIRM: <http://tomcat.apache.org/security-5.html>

CONFIRM: <http://svn.apache.org/viewvc?rev=892815&view=rev>

XF: <http://xforce.iss.net/xforce/xfdb/55855>

BID: <http://www.securityfocus.com/bid/37944>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/509148/100/0/threaded>

UBUNTU: <http://ubuntu.com/usn/usn-899-1>

CONFIRM: <http://svn.apache.org/viewvc?rev=902650&view=rev>

SECTRAK: <http://securitytracker.com/id?1023505>

SECUNIA: <http://secunia.com/advisories/38541>

SECUNIA: <http://secunia.com/advisories/38346>

SECUNIA: <http://secunia.com/advisories/38316>

CVE Reference: [CVE-2009-2693](#)

• **CVE-2009-2901 Apache CVSS 2.0 Score = 4.3**

The autodeployment process in Apache Tomcat 5.5.0 through 5.5.28 and 6.0.0 through 6.0.20, when autoDeploy is enabled, deploys appBase files that remain from a failed undeploy, which might allow remote attackers to bypass intended authentication requirements via HTTP requests.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/0213>

CONFIRM: <http://tomcat.apache.org/security-6.html>

CONFIRM: <http://tomcat.apache.org/security-5.html>

CONFIRM: <http://svn.apache.org/viewvc?rev=902650&view=rev>

CONFIRM: <http://svn.apache.org/viewvc?rev=892815&view=rev>

XF: <http://xforce.iss.net/xforce/xfdb/55856>

BID: <http://www.securityfocus.com/bid/37942>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/509151/100/0/threaded>

UBUNTU: <http://ubuntu.com/usn/usn-899-1>

SECTRAK: <http://securitytracker.com/id?1023503>

SECUNIA: <http://secunia.com/advisories/38541>

SECUNIA: <http://secunia.com/advisories/38346>

SECUNIA: <http://secunia.com/advisories/38316>

CVE Reference: [CVE-2009-2901](#)

• **CVE-2009-2902 Apache CVSS 2.0 Score = 4.3**

Directory traversal vulnerability in Apache Tomcat 5.5.0 through 5.5.28 and 6.0.0 through 6.0.20 allows remote attackers to delete work-directory files via directory traversal sequences in a WAR filename, as demonstrated by the ...war filename.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/55857>

VUPEN: <http://www.vupen.com/english/advisories/2010/0213>

BID: <http://www.securityfocus.com/bid/37945>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/509150/100/0/threaded>

UBUNTU: <http://ubuntu.com/usn/usn-899-1>

CONFIRM: <http://tomcat.apache.org/security-6.html>

CONFIRM: <http://tomcat.apache.org/security-5.html>

CONFIRM: <http://svn.apache.org/viewvc?rev=902650&view=rev>

CONFIRM: <http://svn.apache.org/viewvc?rev=892815&view=rev>

SECTRAK: <http://securitytracker.com/id?1023504>

SECUNIA: <http://secunia.com/advisories/38541>

SECUNIA: <http://secunia.com/advisories/38346>

SECUNIA: <http://secunia.com/advisories/38316>

CVE Reference: [CVE-2009-2902](#)

• **CVE-2005-4884 Oracle CVSS 2.0 Score = 6.8**

Unspecified vulnerability in the Oracle OLAP component in Oracle Database Server 10.1.0.4 (10g) allows remote authenticated attackers to affect availability via unknown vectors, aka DB02.

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

References:

CONFIRM: <http://www.oracle.com/technology/deploy/security/pdf/cpujul2005.html>

CVE Reference: [CVE-2005-4884](#)

• **CVE-2009-4183 HP CVSS 2.0 Score = 4.6**

Unspecified vulnerability in HP OpenView Storage Data Protector 6.00 and 6.10 allows local users to obtain unspecified "access" via unknown vectors.

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

References:

BID: <http://www.securityfocus.com/bid/37964>

OSVDB: <http://www.osvdb.org/61955>

SECUNIA: <http://secunia.com/advisories/38306>

HP: <http://marc.info/?l=bugtraq&m=126461112019142&w=2>

HP: <http://marc.info/?l=bugtraq&m=126461112019142&w=2>

CVE Reference: [CVE-2009-4183](#)

• **CVE-2010-0462 IBM CVSS 2.0 Score = 6.5**

Heap-based buffer overflow in IBM DB2 9.7 and 9.7.1 on Linux allows remote authenticated users to have an unspecified impact via a SELECT statement that has a long column name generated with the REPEAT function.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/55899>

BID: <http://www.securityfocus.com/bid/37976>

SECTRACK: <http://securitytracker.com/id?1023509>

MISC: <http://intevydis.blogspot.com/2010/01/ibm-db2-97-heap-overflow.html>

CVE Reference: [CVE-2010-0462](#)

• **CVE-2010-0140 Cisco CVSS 2.0 Score = 10.0**

Multiple unspecified vulnerabilities in the web server in Cisco Unified MeetingPlace 7 before 7.0(2.3) hotfix 5F, 6 before 6.0.639.3, and possibly 5 allow remote attackers to create (1) user or (2) administrator accounts via a crafted URL in a request to the internal interface, aka Bug IDs CSCtc59231 and CSCtd40661. Per: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b1490b.shtml Affected Products Vulnerable Products Cisco Unified MeetingPlace versions 5, 6, and 7 are each affected by at least one of the vulnerabilities described in this document.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b1490b.shtml

BID: <http://www.securityfocus.com/bid/37965>

CVE Reference: [CVE-2010-0140](#)

• **CVE-2010-0139 Cisco CVSS 2.0 Score = 9.0**

Cisco Unified MeetingPlace 7 before 7.0(2.3) hotfix 5F, 6 before 6.0.639.2, and possibly 5 does not properly validate SQL commands, which allows remote attackers to create, modify, or delete data in a database via unspecified vectors, aka Bug ID CSCtc39691.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b1490b.shtml

BID: <http://www.securityfocus.com/bid/37965>

CVE Reference: [CVE-2010-0139](#)

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