

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

Application attacks worry ISP's. Fixes for Iexpl. holes. How to browse safely. Call for rules on Cloud privacy and security.

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

• Application-level attacks biggest concern for ISPs

IP network operators believe that distributed denial-of-service (DDoS) attacks against services and applications will cause them the most problems during the next 12 months, according to an annual report released Tuesday by network security firm Arbor Networks.

The fifth-annual report, which surveyed 132 respondents from North America, South America, Europe, Africa and Asia, found that 35 percent of respondents believe that service and application-level attacks, which are designed to exploit service weaknesses in vulnerable backend infrastructures, will cause the most disruptions this year, the report states. Botnets were the second largest operational threat, rated the primary concern for 21 percent of respondents. sc Magazine

Full Story :

http://www.scmagazineus.com/application-level-attacks-biggest-concern-for-isps/article/161758/?utm_source=feedb

• Microsoft fixes 8 IE holes, including one used in attacks

Microsoft on Thursday issued a cumulative critical patch for Internet Explorer that fixes eight vulnerabilities, including a hole targeted in the China-based attacks on Google and other U.S. companies.

The security update is rated critical for all supported releases of IE 5, 6, 7, and 8, according to the advisory. The more severe vulnerabilities could allow remote code execution if a user views a malicious Web page using IE, it said.

This IE security update was already planned for release on the next scheduled Patch Tuesday (February 9), Jerry Bryant, senior security program manager at Microsoft, said in a blog post. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-10439004-245.html

• Browse safely with Internet Explorer

Unless you're brand new-to using computers, the recent news that an Internet Explorer hole was exploited in China-based attacks against Google Gmail users and dozens of high-tech companies was no surprise.

Lately, malicious software has increasingly targeted holes in media players such as Adobe's Flash Player and Reader PDF software, so the Chinese attack on IE is in some ways a throwback. Many tech pundits have responded by recommending against using Internet Explorer at all. The free and easy availability of alternative browsers such as Firefox, Opera, Apple's Safari, and Google's own Chrome would appear to make this sound advice. Cnet Security

Full Story :

http://news.cnet.com/8301-13880_3-10436478-68.html

• Microsoft urges laws to boost trust in the cloud

Microsoft is so concerned about the future of cloud computing that it's urging the government to step in.

In a speech Wednesday, Microsoft general counsel and senior vice president Brad Smith called on government and business to shore up confidence in cloud computing by tackling issues of privacy and security--two major concerns that have been voiced about the cloud.

During his keynote speech to the Brookings Institution's "Cloud Computing for Business and Society" form, Smith also appealed to Washington to pass new laws and update existing ones to address problems such as computer fraud and cyberattacks as more businesses and consumers hop onto the cloud. Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-10437844-83.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• 13742 Oracle Database Server - Listener component unspecified Vulnerability (jan-2010/CVE-2010-0071)

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/cpujan2010.html>

* CERT: TA10-012A

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

* BID: 37728

<http://www.securityfocus.com/bid/37728>

* SECTRAK: 1023436

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

* VUPEN: VUPEN/ADV-2010-0102

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

CVE Reference:

CVE-2010-0071 (cve.mitre.org, nvd.nist.gov)

• 13743 Oracle Database Server - Oracle OLAP component unspecified Vulnerability (jan-2010/CVE-2009-3415)

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:

- * BID: 37729
<http://www.securityfocus.com/bid/37729>
- * 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-2009-3415 (cve.mitre.org, nvd.nist.gov)

• **13745 Oracle Database Server - Oracle Data Pump component unspecified Vulnerability (jan-2010/CVE-2009-3411)**

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

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

References:

- * BID: 37743
<http://www.securityfocus.com/bid/37743>
- * 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-2009-3411 (cve.mitre.org, nvd.nist.gov)

• **13746 Oracle Database Server - Oracle Spatial component unspecified Vulnerability (jan-2010/CVE-2009-3414)**

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

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

References:

- * BID: 37730
<http://www.securityfocus.com/bid/37730>
- * 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-2009-3414 (cve.mitre.org, nvd.nist.gov)

• **13747 Oracle Database Server - Logical Standby component unspecified Vulnerability (jan-2010/CVE-2009-1996)**

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

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

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-2009-1996 (cve.mitre.org, nvd.nist.gov)

• 18683 Multiple Vulnerabilities in the IOS FTP Server (cisco-sa-20070509-iosftp) (CVE-2007-2587)

The IOS FTP Server allows remote authenticated users to cause a denial of service (IOS reload) via unspecified vectors involving transferring files.

The IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the IOS FTP Server service are unaffected by these vulnerabilities.

This vulnerability does not apply to the IOS FTP Client feature.

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

References:

* CISCO: cisco-sa-20070509-iosftp

<http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml>

* CISCO: 20070509 Multiple Vulnerabilities in the IOS FTP Server

http://www.cisco.com/en/US/products/products_security_advisory09186a00808399d0.shtml

* BID: 23885

<http://www.securityfocus.com/bid/23885>

* OVAL: oval:org.mitre.oval:def:5444

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5444>

* VUPEN: ADV-2007-1749

<http://www.frsirt.com/english/advisories/2007/1749>

* OSVDB: 35335

<http://www.osvdb.org/35335>

* SECTRACK: 1018030

<http://www.securitytracker.com/id?1018030>

* SECUNIA: 25199

<http://secunia.com/advisories/25199>

* XF: cisco-ios-ftpserver-dos(34196)

<http://xforce.iss.net/xforce/xfdb/34196>

CVE Reference:

CVE-2007-2587 (cve.mitre.org, nvd.nist.gov)

• 18684 Apache mod_ssl CRL Handling Off-By-One Buffer Overflow Vulnerability

Apache's mod_ssl is prone to an off-by-one buffer overflow condition.

The vulnerability arising in the mod_ssl CRL verification callback allows for potential memory corruption when a malicious CRL is handled.

An attacker may exploit this issue to trigger a denial-of-service condition. Presumably, arbitrary code execution may be possible as well.

The vulnerability has been reported in version 2.0.35 through 2.0.37, 2.0.39, 2.0.40, and in version 2.0.42 through 2.0.54.

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

References:

* MISC:

https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=163013

* DEBIAN: DSA-805

<http://www.debian.org/security/2005/dsa-805>

* HP: HPSBUX02074
<http://www.securityfocus.com/archive/1/archive/1/428138/100/0/threaded>
* MANDRAKE: MDKSA-2005:129
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:129>
* REDHAT: RHSA-2005:582
<http://rhn.redhat.com/errata/RHSA-2005-582.html>
* SUNALERT: 102198
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102198-1>
* SUSE: SUSE-SA:2005:046
http://www.novell.com/linux/security/advisories/2005_46_apache.html
* SUSE: SUSE-SR:2005:018
http://www.novell.com/linux/security/advisories/2005_18_sr.html
* TRUSTIX: TSLSA-2005-0059
<http://lists.trustix.org/pipermail/tsl-announce/2005-October/000354.html>
* BID: 14366
<http://www.securityfocus.com/bid/14366>
* VUPEN: ADV-2006-0789
<http://www.frsirt.com/english/advisories/2006/0789>
* SECUNIA: 19072
<http://secunia.com/advisories/19072>
* SECUNIA: 19185
<http://secunia.com/advisories/19185>
* SREASON: 604
<http://securityreason.com/securityalert/604>

CVE Reference:

CVE-2005-1268 (cve.mitre.org, nvd.nist.gov)

• 18685 Vulnerability in Internet Explorer Could Allow Remote Code Execution (979352) (CVE-2010-0249) (Remote File Checking)

Microsoft is investigating reports of limited, targeted attacks against customers of Internet Explorer 6, using a vulnerability in Internet Explorer.

The investigation so far has shown that Internet Explorer 5.01 Service Pack 4 on Microsoft Windows 2000 Service Pack 4 is not affected, and that Internet Explorer 6 Service Pack 1 on Microsoft Windows 2000 Service Pack 4, and Internet Explorer 6, Internet Explorer 7 and Internet Explorer 8 on supported editions of Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2 are vulnerable.

The vulnerability exists as an invalid pointer reference within Internet Explorer. It is possible under certain conditions for the invalid pointer to be accessed after an object is deleted. In a specially-crafted attack, in attempting to access a freed object, Internet Explorer can be caused to allow remote code execution.

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

References:

* CONFIRM:
<http://blogs.technet.com/msrc/archive/2010/01/14/security-advisory-979352.aspx>
* CONFIRM:
<http://www.microsoft.com/technet/security/advisory/979352.msp>
* MSKB: 979352
<http://support.microsoft.com/kb/979352>
* CERT-VN: VU#492515
<http://www.kb.cert.org/vuls/id/492515>
* BID: 37815
<http://www.securityfocus.com/bid/37815>
* SECTRACK: 1023462
<http://securitytracker.com/id?1023462>

CVE Reference:

CVE-2010-0249 (cve.mitre.org, nvd.nist.gov)

• 18686 Microsoft Project Memory Validation Vulnerability (MS09-074/967183) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Project handles specially crafted Project 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.

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

References:

- * MS: MS09-074
<http://www.microsoft.com/technet/security/Bulletin/MS09-074.msp>
- * BID: 37211
<http://www.securityfocus.com/bid/37211>
- * VUPEN: VUPEN/ADV-2009-3439
<http://www.vupen.com/english/advisories/2009/3439>

CVE Reference:

CVE-2009-0102 (cve.mitre.org, nvd.nist.gov)

• 18687 WordPad and Office Text converter Memory Corruption Vulnerability (MS09-073/975539) (Remote File Checking)

A remote code execution vulnerability exists in the way that text converters in Microsoft WordPad and Microsoft Office Word process memory when a user opens a specially crafted Word 97 file.

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

References:

- * IDEFENSE: 20091208 Microsoft WordPad Word97 Converter Integer Overflow Vulnerability
<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=834>
- * CONFIRM:
<http://support.avaya.com/css/P8/documents/100070184>
- * MS: MS09-073
<http://www.microsoft.com/technet/security/Bulletin/MS09-073.msp>
- * BID: 37216
<http://www.securityfocus.com/bid/37216>

CVE Reference:

CVE-2009-2506 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-0378 Microsoft CVSS 2.0 Score = 9.3

Use-after-free vulnerability in Adobe Flash Player 6.0.79, as distributed in Microsoft Windows XP SP2 and SP3, allows remote attackers to execute arbitrary code by unloading a Flash object that is currently being accessed by a script, leading to memory corruption, aka a "Movie Unloading Vulnerability." Per: <http://cwe.mitre.org/data/definitions/416.html>
CWE-416 Use-After Free Vulnerability

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

References:

- CERT-VN: <http://www.kb.cert.org/vuls/id/204889>
- CONFIRM: <http://www.microsoft.com/technet/security/advisory/979267.msp>
- SECTRACK: <http://securitytracker.com/id?1023435>
- MISC: http://secunia.com/secunia_research/2007-77/
- SECUNIA: <http://secunia.com/advisories/27105>

CVE Reference: [CVE-2010-0378](http://cve.mitre.org)

• CVE-2010-0379 Microsoft CVSS 2.0 Score = 9.3

Multiple unspecified vulnerabilities in the Macromedia Flash ActiveX control in Adobe Flash Player 6, as distributed in Microsoft Windows XP SP2 and SP3, might allow remote attackers to execute arbitrary code via unspecified vectors that are not related to the use-after-free "Movie Unloading Vulnerability" (CVE-2010-0378). NOTE: due to lack of details, it is not clear whether this overlaps any other CVE item.

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

References:

CONFIRM: <http://www.microsoft.com/technet/security/advisory/979267.msp>

SECTRAK: <http://securitytracker.com/id?1023435>

SECUNIA: <http://secunia.com/advisories/27105>

CVE Reference: [CVE-2010-0379](#)

• **CVE-2010-0232 Microsoft CVSS 2.0 Score = 6.6**

The kernel in Microsoft Windows NT 3.1 through Windows 7, including Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, and Windows Server 2008 Gold and SP2, when access to 16-bit applications is enabled on a 32-bit x86 platform, does not properly validate certain BIOS calls, which allows local users to gain privileges by crafting a VDM_TIB data structure in the Thread Environment Block (TEB), and then calling the NtVdmControl function to start the Windows Virtual DOS Machine (aka NTVDM) subsystem, leading to improperly handled exceptions involving the #GP trap handler (aka nt!KiTrap0D).

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/55742>

VUPEN: <http://www.vupen.com/english/advisories/2010/0179>

BID: <http://www.securityfocus.com/bid/37864>

CONFIRM: <http://www.microsoft.com/technet/security/advisory/979682.msp>

SECTRAK: <http://securitytracker.com/id?1023471>

SECUNIA: <http://secunia.com/advisories/38265>

FULLDISC: <http://seclists.org/fulldisclosure/2010/Jan/341>

MISC: <http://lock.cmpxchg8b.com/c0af0967d904cef2ad4db766a00bc6af/KiTrap0D.zip>

MLIST: <http://lists.immunitysec.com/pipermail/dailydave/2010-January/006000.html>

CONFIRM: <http://blogs.technet.com/msrc/archive/2010/01/20/security-advisory-979682-released.aspx>

CVE Reference: [CVE-2010-0232](#)

• **CVE-2009-3999 HP CVSS 2.0 Score = 10.0**

Stack-based buffer overflow in goform/formExportDataLogs in HP Power Manager before 4.2.10 allows remote attackers to execute arbitrary code via a long fileName parameter.

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

References:

BID: <http://www.securityfocus.com/bid/37867>

SECTRAK: <http://securitytracker.com/id?1023470>

MISC: http://secunia.com/secunia_research/2009-47/

SECUNIA: <http://secunia.com/advisories/37280>

HP: <http://marc.info/?l=bugtraq&m=126393370331959&w=2>

HP: <http://marc.info/?l=bugtraq&m=126393370331959&w=2>

CVE Reference: [CVE-2009-3999](#)

• **CVE-2009-4000 HP CVSS 2.0 Score = 7.5**

Directory traversal vulnerability in goform/formExportDataLogs in HP Power Manager before 4.2.10 allows remote attackers to overwrite arbitrary files, and execute arbitrary code, via directory traversal sequences in the fileName parameter.

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

References:

BID: <http://www.securityfocus.com/bid/37873>

SECTRAK: <http://securitytracker.com/id?1023470>

MISC: http://secunia.com/secunia_research/2009-48/

SECUNIA: <http://secunia.com/advisories/37280>

HP: <http://marc.info/?l=bugtraq&m=126393370331959&w=2>

HP: <http://marc.info/?l=bugtraq&m=126393370331959&w=2>

CVE Reference: [CVE-2009-4000](#)

• CVE-2010-0358 IBM CVSS 2.0 Score = 10.0

Heap-based buffer overflow in the server in IBM Lotus Domino 7 and 8.5 FP1 allows remote attackers to cause a denial of service (daemon exit) and possibly have unspecified other impact via a long string in a crafted LDAP message to a TCP port, a different vulnerability than CVE-2009-3087.

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

References:

SECTRAK: <http://securitytracker.com/id?1023456>

MISC: <http://intevydis.com/vd-list.shtml>

MISC: <http://intevydis.blogspot.com/2010/01/lotus-domino-7-probably-8-ldap-heap.html>

CVE Reference: [CVE-2010-0358](#)

• CVE-2009-4003 Adobe CVSS 2.0 Score = 10.0

Multiple integer overflows in Adobe Shockwave Player before 11.5.6.606 allow remote attackers to execute arbitrary code via (1) an unspecified block type in a Shockwave file, leading to a heap-based buffer overflow; and might allow remote attackers to execute arbitrary code via (2) an unspecified 3D block in a Shockwave file, leading to memory corruption; or (3) a crafted 3D model in a Shockwave file, leading to heap memory corruption.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/55759>

VUPEN: <http://www.vupen.com/english/advisories/2010/0171>

BID: <http://www.securityfocus.com/bid/37872>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/509058/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/509055/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/509053/100/0/threaded>

CONFIRM: <http://www.adobe.com/support/security/bulletins/apsb10-03.html>

SECTRAK: <http://securitytracker.com/id?1023481>

MISC: http://secunia.com/secunia_research/2010-1/

MISC: http://secunia.com/secunia_research/2009-63/

MISC: http://secunia.com/secunia_research/2009-62/

SECUNIA: <http://secunia.com/advisories/37888>

CVE Reference: [CVE-2009-4003](#)

• CVE-2010-0361 Sun CVSS 2.0 Score = 10.0

Stack-based buffer overflow in the WebDAV implementation in webservd in Sun Java System Web Server (aka SJWS) 7.0 Update 7 allows remote attackers to cause a denial of service (daemon crash) and possibly have unspecified other impact via a long URI in an HTTP OPTIONS request.

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

References:

MISC: <http://intevydis.blogspot.com/2010/01/sun-java-system-web-server-70u7-webdav.html>

CVE Reference: [CVE-2010-0361](https://cve.mitre.org/cve/2010/0361)

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