ScoutNews
The weekly Security update from the makers of SecureScout
February 05, 2010

2010 Issue #6

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

New approach needed. Growing dangers challenges of cyberwar. Another Internet Explorer flaw under investigation. Google to team up with NSA on cyber defense.

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 says U.S. needs new approach for security**

The United States needs a new approach to secure cyberspace and prevent a "digital Pearl Harbor or 9/11," concludes a new report issued Monday by the Cyber Secure Institute, a nonprofit cybersecurity analysis and advocacy organization.

A new report titled "Cyberwarfare and Cyberterrorism: The Need for a New U.S. Strategic Approach," authored by retired Gen. Eugene Habiger of the U.S. Air Force, concludes that that the public and private sector must deploy secure systems that are properly tested and certified to withstand sophisticated cyberattacks.

In addition, the government must ensure that the privately-owned critical infrastructure systems are secured, as well as coordinate a public awareness campaign to promote personal cybersecurity, such as the use of stronger passwords. SC Magazine

Full Story :
http://www.scmagazineus.com/report-says-us-needs-new-approach-for-security/article/162859/?utm_source=feedbu

- **Government warns of looming cyberthreats**

White House Director of National Intelligence Dennis Blair says the U.S. is severely under the threat of greater cyberattacks but believes we can rise to the challenge.

Blair appeared before a Senate panel on Tuesday to deliver the Annual Threat Assessment of the U.S. Intelligence Community (PDF). A statement of Blair's remarks to the Senate Select Committee on Intelligence was released for the record. While he focused mostly on non-cyberterrorism and similar threats, he led off with a stark report on the growing dangers and challenges of cyberwarfare.

Seeing the recent attacks against Google as a "wake-up call," Blair cautioned those who may treat the problem lightly. He also praised companies who report such incidents as they help Washington better understand the nature of cyberthreats that can affect the entire nation. Cnet Security

Full Story :
http://news.cnet.com/8301-1009_3-10446647-83.html?part=rss&subj=news&tag=2547-1_3-0-20

- **Microsoft investigates new Internet Explorer flaw**

Microsoft said on Wednesday that it is investigating another flaw in Internet Explorer, this time a vulnerability that could result in an unauthorized disclosure of information for users running its browser on older operating systems.

The software maker said in a security advisory that, although it knows of no attacks based on the flaw, the vulnerability could lead to a Web-based attack from either a Web site designed to take advantage of the flaw or from a site that becomes compromised via user-generated text or a malicious ad. Either way, a user would have to actively go to the compromised Web site.

The flaw is separate from the one used to attack Google and other companies, which Microsoft addressed with an "out-of-band" security update last month. Cnet Security

Full Story :
http://news.cnet.com/8301-13860_3-10447081-56.html

- **Report: Google, NSA talk defense partnership**

Google is finalizing an agreement with the National Security Agency to help the search giant ward off cyberattacks, according to the Washington Post.

The electronic surveillance organization is expected to help analyze a cyberattack on Google that the company said originated in China, so that the company can better defend itself against future attacks, the newspaper reported Wednesday. The arrangement is reportedly being designed to allow the two groups to share information without violating Google's privacy policies or laws governing online communications.

Google declined to comment on the report, and the NSA did not immediately respond to a request for comment. Cnet Security

Full Story :
http://news.cnet.com/8301-1009_3-10447279-83.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

- **14525 Adobe Acrobat / Reader array boundary issue Vulnerability (CVE-2009-3953) (Remote File Checking)**

The U3D implementation in Adobe Reader and Acrobat 9.x before 9.3, and 8.x before 8.2 on Windows and Mac OS X, might allow attackers to execute arbitrary code via unspecified vectors, related to an "array boundary issue," a different vulnerability than CVE-2009-2994.

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

References:

* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb10-02.html
* SUSE: SUSE-SA:2010:008
http://lists.opensuse.org/opensuse-security-announce/2010-01/msg00009.html
* CERT: TA10-013A
http://www.us-cert.gov/cas/techalerts/TA10-013A.html
* SECTRACK: 1023446
http://www.securitytracker.com/id?1023446
* VUPEN: ADV-2010-0103
http://www.vupen.com/english/advisories/2010/0103

CVE Reference:

CVE-2009-3953 (cve.mitre.org, nvd.nist.gov)

• 14526 Adobe Acrobat / Reader DLL-loading Vulnerability (CVE-2009-3954) (Remote File Checking)

The 3D implementation in Adobe Reader and Acrobat 9.x before 9.3, and 8.x before 8.2 on Windows and Mac OS X, might allow attackers to execute arbitrary code via unspecified vectors, related to a "DLL-loading vulnerability."

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

References:

* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb10-02.html
* SUSE: SUSE-SA:2010:008
http://lists.opensuse.org/opensuse-security-announce/2010-01/msg00009.html
* CERT: TA10-013A
http://www.us-cert.gov/cas/techalerts/TA10-013A.html
* SECTRACK: 1023446
http://www.securitytracker.com/id?1023446
* VUPEN: ADV-2010-0103
http://www.vupen.com/english/advisories/2010/0103

CVE Reference:

CVE-2009-3954 (cve.mitre.org, nvd.nist.gov)

• 14527 Adobe Acrobat / Reader memory corruption Vulnerability (CVE-2009-3955) (Remote File Checking)

Adobe Reader and Acrobat 9.x before 9.3, and 8.x before 8.2 on Windows and Mac OS X, allows remote attackers to execute arbitrary code via a crafted JPC_MS_RGN marker in the Jp2c stream of a JpxDecode encoded data stream, which triggers an integer sign extension that bypasses a sanity check, leading to memory corruption.

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

References:

* IDEFENSE: 20100113 Adobe Reader and Acrobat JpxDecode Memory Corruption Vulnerability
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=836
* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb10-02.html
* SUSE: SUSE-SA:2010:008
http://lists.opensuse.org/opensuse-security-announce/2010-01/msg00009.html
* CERT: TA10-013A
http://www.us-cert.gov/cas/techalerts/TA10-013A.html
* BID: 37757
http://www.securityfocus.com/bid/37757
* SECTRACK: 1023446
http://www.securitytracker.com/id?1023446
* VUPEN: ADV-2010-0103
http://www.vupen.com/english/advisories/2010/0103
* XF: acrobat-reader-jpxdecode-code-exec(55553)
http://xforce.iss.net/xforce/xfdb/55553

CVE Reference:

CVE-2009-3955 (cve.mitre.org, nvd.nist.gov)

• 14528 Adobe Acrobat / Reader script injection Vulnerability (CVE-2009-3956) (Remote File Checking)

The default configuration of Adobe Reader and Acrobat 9.x before 9.3, and 8.x before 8.2 on Windows and Mac OS X, does not properly support the Enhanced Security feature, which has unspecified impact and attack vectors, related to a "script injection vulnerability."

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

References:

* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb10-02.html
* SUSE: SUSE-SA:2010:008
http://lists.opensuse.org/opensuse-security-announce/2010-01/msg00009.html
* CERT: TA10-013A
http://www.us-cert.gov/cas/techalerts/TA10-013A.html
* SECTRACK: 1023446
http://www.securitytracker.com/id?1023446
* VUPEN: ADV-2010-0103
http://www.vupen.com/english/advisories/2010/0103

CVE Reference:

CVE-2009-3956 (cve.mitre.org, nvd.nist.gov)

• 14529 Adobe Acrobat / Reader null-pointer dereference Vulnerability (CVE-2009-3957) (Remote File Checking)

Adobe Reader and Acrobat 9.x before 9.3, and 8.x before 8.2 on Windows and Mac OS X, might allow attackers to cause a denial of service (NULL pointer dereference) via unspecified vectors.

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

References:

* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb10-02.html
* SUSE: SUSE-SA:2010:008
http://lists.opensuse.org/opensuse-security-announce/2010-01/msg00009.html
* CERT: TA10-013A
http://www.us-cert.gov/cas/techalerts/TA10-013A.html
* SECTRACK: 1023446
http://www.securitytracker.com/id?1023446
* VUPEN: ADV-2010-0103
http://www.vupen.com/english/advisories/2010/0103

CVE Reference:

CVE-2009-3957 (cve.mitre.org, nvd.nist.gov)

• 14530 Adobe Acrobat / Reader buffer overflow Vulnerability (CVE-2009-3958) (Remote File Checking)

Buffer overflow in the Download Manager in Adobe Reader and Acrobat 9.x before 9.3, and 8.x before 8.2 on Windows and Mac OS X, might allow attackers to execute arbitrary code via unspecified vectors.

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

References:

* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb10-02.html
* SUSE: SUSE-SA:2010:008
http://lists.opensuse.org/opensuse-security-announce/2010-01/msg00009.html
* CERT: TA10-013A
http://www.us-cert.gov/cas/techalerts/TA10-013A.html
* SECTRACK: 1023446
http://www.securitytracker.com/id?1023446
* VUPEN: ADV-2010-0103
http://www.vupen.com/english/advisories/2010/0103

CVE Reference:

CVE-2009-3958 (cve.mitre.org, nvd.nist.gov)

• 14531 Adobe Acrobat / Reader integer overflow Vulnerability (CVE-2009-3959) (Remote File Checking)

Integer overflow in the U3D implementation in Adobe Reader and Acrobat 9.x before 9.3, and 8.x before 8.2 on Windows and Mac OS X, might allow attackers to execute arbitrary code via unspecified vectors.

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

References:

* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb10-02.html
* SUSE: SUSE-SA:2010:008
http://lists.opensuse.org/opensuse-security-announce/2010-01/msg00009.html
* CERT: TA10-013A
http://www.us-cert.gov/cas/techalerts/TA10-013A.html
* SECTRACK: 1023446
http://www.securitytracker.com/id?1023446
* VUPEN: ADV-2010-0103
http://www.vupen.com/english/advisories/2010/0103

CVE Reference:

CVE-2009-3959 (cve.mitre.org, nvd.nist.gov)

• 14532 Adobe Acrobat / Reader use-after-free Vulnerability (CVE-2009-4324) (Remote File Checking)

Use-after-free vulnerability in the Doc.media.newPlayer method in Multimedia.api in Adobe Reader and Acrobat 9.x before 9.3, and 8.x before 8.2 on Windows and Mac OS X, allows remote attackers to execute arbitrary code via a crafted PDF file using ZLib compressed streams, as exploited in the wild in December 2009.

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

References:

* MISC:
http://blogs.adobe.com/psirt/2009/12/new_adobe_reader_and_acrobat_v.html
* MISC:
http://contagiodump.blogspot.com/2009/12/virustotal-httpwww.html
* MISC:
http://www.metasploit.com/redmine/projects/framework/repository/revisions/7881/entry/modules/exploits/windows/fileforma
* MISC:
http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20091214
* MISC:
http://www.symantec.com/connect/blogs/zero-day-xmas-present
* CONFIRM:
http://www.adobe.com/support/security/advisories/apsa09-07.html
* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb10-02.html
* SUSE: SUSE-SA:2010:008
http://lists.opensuse.org/opensuse-security-announce/2010-01/msg00009.html
* CERT: TA10-013A
http://www.us-cert.gov/cas/techalerts/TA10-013A.html
* CERT-VN: VU#508357
http://www.kb.cert.org/vuls/id/508357
* BID: 37331
http://www.securityfocus.com/bid/37331
* OSVDB: 60980
http://osvdb.org/60980
* SECUNIA: 37690
http://secunia.com/advisories/37690
* VUPEN: ADV-2009-3518
http://www.vupen.com/english/advisories/2009/3518
* VUPEN: ADV-2010-0103
http://www.vupen.com/english/advisories/2010/0103
* XF: acro-reader-unspecifed-code-execution(54747)
http://xforce.iss.net/xforce/xfdb/54747

CVE Reference:

CVE-2009-4324 (cve.mitre.org, nvd.nist.gov)

• 14533 Adobe Acrobat / Reader Denial of Service Vulnerability (CVE-2007-0048) (Remote File Checking)

Adobe Acrobat Reader Plugin before 8.0.0, and possibly the plugin distributed with Adobe Reader 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2, when used with Internet Explorer, Google Chrome, or Opera, allows remote attackers to cause a denial of service (memory consumption) via a long sequence of # (hash) characters appended to a PDF URL, related to a "cross-site scripting issue."

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

References:

* BUGTRAQ: 20070103 Adobe Acrobat Reader Plugin - Multiple Vulnerabilities
http://www.securityfocus.com/archive/1/archive/1/455801/100/0/threaded
* MISC:
http://events.ccc.de/congress/2006/Fahrplan/attachments/1158-Subverting_Ajax.pdf
* MISC:
http://www.wisec.it/vulns.php?page=9
* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb07-01.html
* CONFIRM:
http://googlechromereleases.blogspot.com/2009/01/stable-beta-update-yahoo-mail-and.html
* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb09-15.html
* GENTOO: GLSA-200701-16
http://security.gentoo.org/glsa/glsa-200701-16.xml
* SUSE: SUSE-SA:2007:011
http://lists.suse.com/archive/suse-security-announce/2007-Jan/0012.html
* CERT: TA09-286B
http://www.us-cert.gov/cas/techalerts/TA09-286B.html
* SECTRACK: 1023007
http://securitytracker.com/id?1023007
* VUPEN: ADV-2007-0032
http://www.frsirt.com/english/advisories/2007/0032
* OSVDB: 31596
http://osvdb.org/31596
* SECTRACK: 1017469
http://securitytracker.com/id?1017469
* SECUNIA: 23812
http://secunia.com/advisories/23812
* SECUNIA: 23882
http://secunia.com/advisories/23882
* SECUNIA: 33754
http://secunia.com/advisories/33754
* SREASON: 2090
http://securityreason.com/securityalert/2090
* VUPEN: ADV-2009-2898
http://www.vupen.com/english/advisories/2009/2898
* XF: adobe-acrobat-character-dos(31273)
http://xforce.iss.net/xforce/xfdb/31273

CVE Reference:

CVE-2007-0048 (cve.mitre.org, nvd.nist.gov)

• 14534 Adobe Acrobat / Reader cross-site scripting Vulnerability (CVE-2007-0045) (Remote File Checking)

Multiple cross-site scripting (XSS) vulnerabilities in Adobe Acrobat Reader Plugin before 8.0.0, and possibly the plugin distributed with Adobe Reader 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2, for Mozilla Firefox, Microsoft Internet Explorer 6 SP1, Google Chrome, Opera 8.5.4 build 770, and Opera 9.10.8679 on Windows allow remote attackers to inject arbitrary JavaScript and conduct other attacks via a .pdf URL with a javascript: or res: URI with (1) FDF, (2) XML, and (3) XFDF AJAX parameters, or (4) an arbitrarily named name=URI anchor identifier, aka "Universal XSS (UXSS)."

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

References:

* BUGTRAQ: 20070103 Adobe Acrobat Reader Plugin - Multiple Vulnerabilities
http://www.securityfocus.com/archive/1/archive/1/455801/100/0/threaded
* BUGTRAQ: 20070103 RE: [WEB SECURITY] Universal XSS with PDF files: highly dangerous
http://www.securityfocus.com/archive/1/455836/100/0/threaded
* BUGTRAQ: 20070103 Re: Universal XSS with PDF files: highly dangerous
http://www.securityfocus.com/archive/1/455800/100/0/threaded

* BUGTRAQ: 20070103 Re: [WEB SECURITY] Universal XSS with PDF files: highly dangerous
http://www.securityfocus.com/archive/1/455831/100/0/threaded
* BUGTRAQ: 20070103 Universal XSS with PDF files: highly dangerous
http://www.securityfocus.com/archive/1/455790/100/0/threaded
* BUGTRAQ: 20070104 Universal PDF XSS After Party
http://www.securityfocus.com/archive/1/archive/1/455906/100/0/threaded
* MISC:
http://events.ccc.de/congress/2006/Fahrplan/attachments/1158-Subverting_Ajax.pdf
* MISC:
http://www.wisec.it/vulns.php?page=9
* MISC:
http://www.disenchant.ch/blog/hacking-with-browser-plugins/34
* MISC:
http://www.gnucitizen.org/blog/universal-pdf-xss-after-party
* CONFIRM:
http://www.gnucitizen.org/blog/danger-danger-danger/
* CONFIRM:
http://www.adobe.com/support/security/advisories/apsa07-01.html
* CONFIRM:
http://www.adobe.com/support/security/advisories/apsa07-02.html
* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb07-01.html
* CONFIRM:
http://www.mozilla.org/security/announce/2007/mfsa2007-02.html
* CONFIRM:
http://googlechromereleases.blogspot.com/2009/01/stable-beta-update-yahoo-mail-and.html
* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb09-15.html
* GENTOO: GLSA-200701-16
http://security.gentoo.org/glsa/glsa-200701-16.xml
* HP: HPSBUX02153
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00771742
* REDHAT: RHSA-2007:0017
https://rhn.redhat.com/errata/RHSA-2007-0017.html
* REDHAT: RHSA-2007:0021
http://www.redhat.com/support/errata/RHSA-2007-0021.html
* SLACKWARE: SSA:2007-066-05
http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.338131
* SUNALERT: 102847
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102847-1
* SUSE: SUSE-SA:2007:011
http://lists.suse.com/archive/suse-security-announce/2007-Jan/0012.html
* CERT: TA09-286B
http://www.us-cert.gov/cas/techalerts/TA09-286B.html
* CERT-VN: VU#815960
http://www.kb.cert.org/vuls/id/815960
* BID: 21858
http://www.securityfocus.com/bid/21858
* SECTRACK: 1023007
http://securitytracker.com/id?1023007
* VUPEN: ADV-2007-0032
http://www.frsirt.com/english/advisories/2007/0032
* VUPEN: ADV-2007-0957
http://www.frsirt.com/english/advisories/2007/0957
* SECTRACK: 1017469
http://securitytracker.com/id?1017469
* SECUNIA: 23483
http://secunia.com/advisories/23483
* SECUNIA: 23691
http://secunia.com/advisories/23691
* SECUNIA: 23812
http://secunia.com/advisories/23812
* SECUNIA: 23877
http://secunia.com/advisories/23877
* SECUNIA: 23882
http://secunia.com/advisories/23882
* SECUNIA: 24533
http://secunia.com/advisories/24533
* SECUNIA: 24457

http://secunia.com/advisories/24457
* SECUNIA: 33754
http://secunia.com/advisories/33754
* SREASON: 2090
http://securityreason.com/securityalert/2090
* VUPEN: ADV-2009-2898
http://www.vupen.com/english/advisories/2009/2898
* XF: adobe-acrobat-pdf-xss(31271)
http://xforce.iss.net/xforce/xfdb/31271

CVE Reference:

CVE-2007-0045 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- **CVE-2010-0555 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 5.01 SP4, 6, 6 SP1, 7, and 8 does not prevent rendering of non-HTML local files as HTML documents, which allows remote attackers to bypass intended access restrictions and read arbitrary files via vectors involving the product's use of text/html as the default content type for files that are encountered after a redirection, aka the URLMON sniffing vulnerability, a variant of CVE-2009-1140 and related to CVE-2008-1448.

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

References:

BID: http://www.securityfocus.com/bid/38056

BID: http://www.securityfocus.com/bid/38055

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/509345/100/0/threaded

MISC: http://www.microsoft.com/technet/security/advisory/980088.mspx

MISC: http://www.coresecurity.com/content/internet-explorer-dynamic-object-tag

MISC: http://isc.sans.org/diary.html?n&storyid=8152

MISC: http://blogs.technet.com/msrc/archive/2010/02/03/security-advisory-980088-released.aspx

CVE Reference: CVE-2010-0555

- **CVE-2010-0255 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 5.01 SP4, 6, 6 SP1, 7, and 8 does not prevent rendering of non-HTML local files as HTML documents, which allows remote attackers to bypass intended access restrictions and read arbitrary files via vectors involving JavaScript exploit code that constructs a reference to a file://127.0.0.1 URL, aka the dynamic OBJECT tag vulnerability, as demonstrated by obtaining the data from an index.dat file, a variant of CVE-2009-1140 and related to CVE-2008-1448.

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

References:

BID: http://www.securityfocus.com/bid/38056

BID: http://www.securityfocus.com/bid/38055

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/509345/100/0/threaded

CONFIRM: http://www.microsoft.com/technet/security/advisory/980088.mspx

MISC: http://www.coresecurity.com/content/internet-explorer-dynamic-object-tag

MISC: http://isc.sans.org/diary.html?n&storyid=8152

CONFIRM: http://blogs.technet.com/msrc/archive/2010/02/03/security-advisory-980088-released.aspx

CVE Reference: CVE-2010-0255

- **CVE-2003-1582 Microsoft CVSS 2.0 Score = 2.6**

Microsoft Internet Information Services (IIS) 6.0, when DNS resolution is enabled for client IP addresses, allows remote attackers to inject arbitrary text into log files via an HTTP request in conjunction with a crafted DNS response, as demonstrated by injecting XSS sequences, related to an "Inverse Lookup Log Corruption (ILLC)" issue.

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

References:

BUGTRAQ: http://www.securityfocus.com/archive/1/313867

CVE Reference: CVE-2003-1582

- **CVE-2010-0010 Apache CVSS 2.0 Score = 6.8**

Integer overflow in the ap_proxy_send_fb function in proxy/proxy_util.c in mod_proxy in the Apache HTTP Server before 1.3.42 on 64-bit platforms allows remote origin servers to cause a denial of service (daemon crash) or possibly execute arbitrary code via a large chunk size that triggers a heap-based buffer overflow.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/55941

VUPEN: http://www.vupen.com/english/advisories/2010/0240

BID: http://www.securityfocus.com/bid/37966

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/509185/100/0/threaded

MISC: http://site.pi3.com.pl/adv/mod_proxy.txt

SECUNIA: http://secunia.com/advisories/38319

MISC: http://packetstormsecurity.org/1001-exploits/modproxy-overflow.txt

CONFIRM: http://httpd.apache.org/dev/dist/CHANGES_1.3.42

MISC: http://blog.pi3.com.pl/?p=69

FULLDISC: http://archives.neohapsis.com/archives/fulldisclosure/2010-01/0589.html

CVE Reference: CVE-2010-0010

- **CVE-2003-1580 Apache CVSS 2.0 Score = 4.3**

The Apache HTTP Server 2.0.44, when DNS resolution is enabled for client IP addresses, uses a logging format that does not identify whether a dotted quad represents an unresolved IP address, which allows remote attackers to spoof IP addresses via crafted DNS responses containing numerical top-level domains, as demonstrated by a forged 123.123.123.123 domain name, related to an "Inverse Lookup Log Corruption (ILLC)" issue.

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

References:

BUGTRAQ: http://www.securityfocus.com/archive/1/313867

CVE Reference: CVE-2003-1580

- **CVE-2010-0443 HP CVSS 2.0 Score = 6.8**

Unspecified vulnerability in Record Management Services (RMS) before VMS83A_RMS-V1100 for HP OpenVMS on the Alpha platform allows local users to gain privileges via unknown vectors.

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

References:

VUPEN: http://www.vupen.com/english/advisories/2010/0286

HP: http://marc.info/?l=bugtraq&m=126520981100671&w=2

HP: http://marc.info/?l=bugtraq&m=126520981100671&w=2

XF: http://xforce.iss.net/xforce/xfdb/56062

BID: http://www.securityfocus.com/bid/38048

SECUNIA: http://secunia.com/advisories/38366

CVE Reference: CVE-2010-0443

- **CVE-2009-4184 HP CVSS 2.0 Score = 6.2**

Unspecified vulnerability in HP Enterprise Cluster Master Toolkit (ECMT) B.05.00 on HP-UX B.11.23 (11i v2) and HP-UX B.11.31 (11i v3) allows local users to gain access to an Oracle or Sybase database via unknown vectors.

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

References:

VUPEN: http://www.vupen.com/english/advisories/2010/0272

SECTRACK: http://www.securitytracker.com/id?1023523

BID: http://www.securityfocus.com/bid/38035

SECUNIA: http://secunia.com/advisories/38423

HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01894850

HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01894850

CVE Reference: CVE-2009-4184

- **CVE-2009-4185 HP CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in proxy/smhui/getuiinfo in HP System Management Homepage (SMH) before 6.0 allows remote attackers to inject arbitrary web script or HTML via the servercert parameter.

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

References:

VUPEN: http://www.vupen.com/english/advisories/2010/0294

BID: http://www.securityfocus.com/bid/38081

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/509195/100/0/threaded

MISC: http://www.procheckup.com/vulnerability_manager/vulnerabilities/pr09-15

SECUNIA: http://secunia.com/advisories/38341

HP: http://marc.info/?l=bugtraq&m=126529736830358&w=2

HP: http://marc.info/?l=bugtraq&m=126529736830358&w=2

CVE Reference: CVE-2009-4185

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