
HOYT LLC
http://hoytllc.com
Strategic Consulting

Hoyt LLC Audit Report

Device report for 209.20.76.247

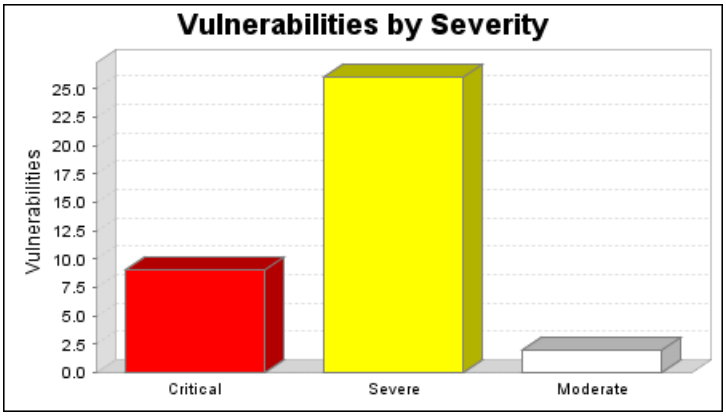
Audited on July 21 2010

1. Executive Summary

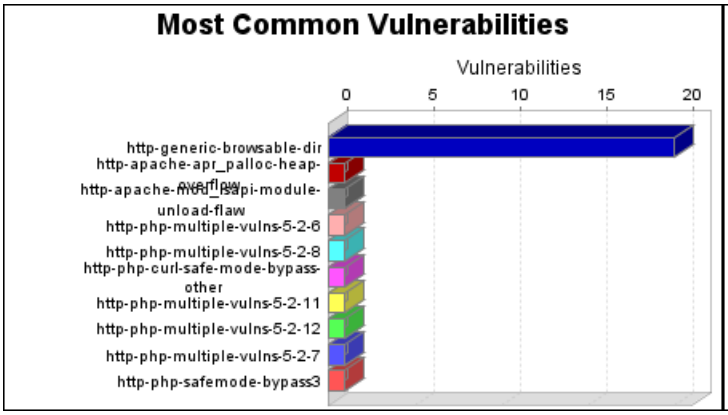
This report represents a security audit performed by Hoyt LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

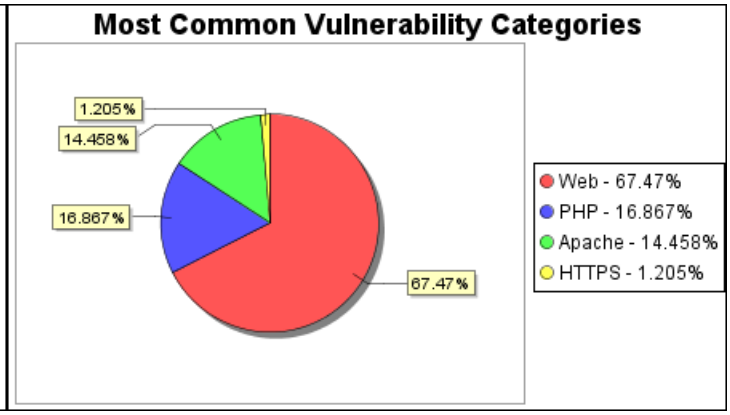
Site Name	Start Time	End Time	Total Time	Status
westsystem.com	July 21, 2010 22:34, EDT	July 21, 2010 22:37, EDT	3 minutes	Success

The audit was performed on one system which was found to be active and was scanned.

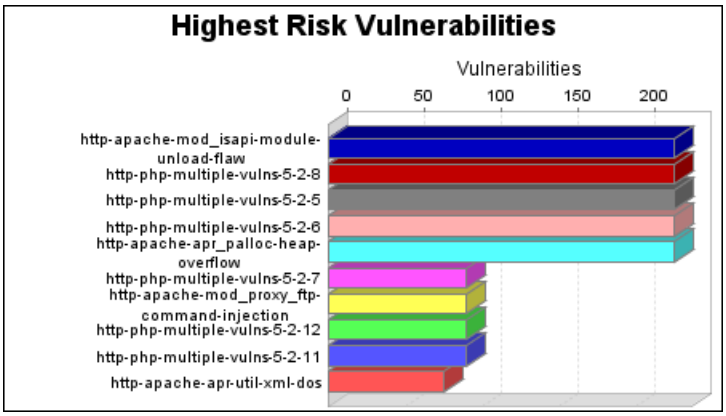


There were 37 vulnerabilities found during this scan. Of these, 9 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 26 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 2 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities.

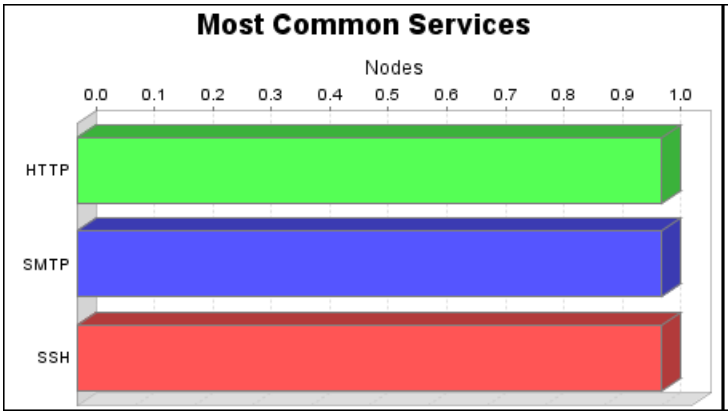


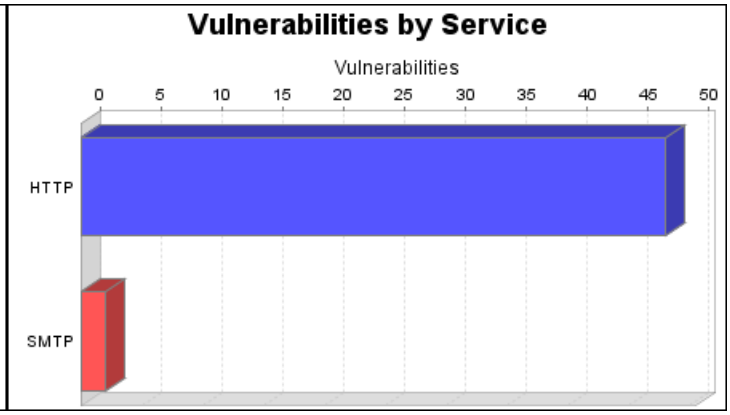


There were 20 occurrences of the http-generic-browsable-dir vulnerability, making it the most common vulnerability. There were 56 vulnerabilities in the Web category, making it the most common vulnerability category.



The http-apache-mod_isapi-module-unload-flaw, http-php-multiple-vulns-5-2-8, http-php-multiple-vulns-5-2-5, http-php-multiple-vulns-5-2-6 and http-apache-apr_palloc-heap-overflow vulnerabilities pose the highest risk to the organization with a risk score of 225. Vulnerability risk scores are calculated by looking at the likelihood of attack and impact, based upon CVSS metrics. The impact and likelihood are then multiplied by the number of instances of the vulnerability to come up with the final risk score.
One operating system was identified during this scan.
There were 3 services found to be running during this scan.





The HTTP, SMTP and SSH services were found on 1 systems, making them the most common services. The HTTP service was found to have the most vulnerabilities during this scan with 48 vulnerabilities.

2. Discovered Systems

Node	Operating System	Risk	Aliases
209.20.76.247	Ubuntu Linux	5.63	•209-20-76-247.slicehost.net •westsystem.com

3. Discovered and Potential Vulnerabilities

3.1. Critical Vulnerabilities

3.1.1. Apache APR apr_palloc Heap Overflow (http-apache-apr_palloc-heap-overflow)

Description:

A flaw in apr_palloc() in the bundled copy of APR could cause heap overflows in programs that try to apr_palloc() a user controlled size. The Apache HTTP Server itself does not pass unsanitized user-provided sizes to this function, so it could only be triggered through some other application which uses apr_palloc() in a vulnerable way.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	35949
CVE	CVE-2009-2412
SECUNIA	36138
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.13.tar.bz2

Many platforms and distributions provide pre-built binary packages for Apache. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.1.2. Apache mod_isapi Module Unload Flaw (http-apache-mod_isapi-module-unload-flaw)

Description:

A flaw was found with within mod_isapi which would attempt to unload the ISAPI dll when it encountered various error states. This could leave the callbacks in an undefined state and result in a segfault. On Windows platforms using mod_isapi, a remote attacker

could send a malicious request to trigger this issue, and as win32 MPM runs only one process, this would result in a denial of service, and potentially allow arbitrary code execution.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	38494
CVE	CVE-2010-0425
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.bz2

Many platforms and distributions provide pre-built binary packages for Apache. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.1.3. PHP Multiple Vulnerabilities Fixed in version 5.2.6 (http-php-multiple-vulns-5-2-6)

Description:

Certain versions of PHP ship with flawed implementations of the init_reauest_info() and escapeshellcmd() functions, the GENERATE_SEED macro, and FastCGI SAPI.

The init_request_info() function does not properly calculate the length of PATH_TRANSLATED due to improper operator precedence handling. This could allow a remote attacker to execute arbitrary code via a crafted URI (CVE-2008-0599).

The FastCGI SAPI contains a stack-based overflow of unknown impact and attack vector (CVE-2008-2050).

The escapeshellcmd API function is vulnerable to an attack of unknown impact via a context-dependent attack (CVE-2008-2051).

The GENERATE_SEED macro can produce a zero seed. This could allow a remote attacker to bypass protection mechanisms via subsequent values based on the initial seed (CVE-2008-2107, CVE-2008-2108).

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	29009
CVE	CVE-2008-0599
CVE	CVE-2008-2050
CVE	CVE-2008-2051
CVE	CVE-2008-2107
CVE	CVE-2008-2108
SECUNIA	30048

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.2.6.tar.gz/from/a/mirror
Upgrade to PHP v5.2.6 (released on May 1st, 2008).

3.1.4. PHP Multiple Vulnerabilities Fixed in version 5.2.8 (http-php-multiple-vulns-5-2-8)

Description:

Certain versions of PHP ship with a vulnerable version of the PCRE library. This could allow a context-dependent attacker to cause a denial of service (crash) via a specially crafted regular expression. (CVE-2008-2371)

The imageloadfont() function could allow a context-dependent attacker to cause a denial of service (crash) via a crafted font file. (CVE-2008-3658)

The memnstr() function could allow a context-dependent attacker to cause a denial of service (crash) via the delimiter argument to the explode function. (CVE-2008-3659)

Certain versions of PHP, when used as a FastCGI module, could allow a remote attacker to cause a denial of service (crash). (CVE-2008-3660)

Certain versions of PHP ship with a heap-based buffer overflow in the mbstring extension. This could allow context-dependent attackers to execute arbitrary code via a crafted string. (CVE-2008-5557)

The page_uid and page_gid global variables are not properly initialized for use by the SAPI php_getuid function. This could allow context-dependent attackers to bypass safe_mode restrictions via variable settings. (CVE-2008-5624)

Certain versions of PHP do not enforce the error_log safe_mode restrictions when safe_mode is enabled. This could allow context-dependent attackers to write to arbitrary files. (CVE-2008-5625)

The ZipArchive::extractTo function in certain versions of PHP contains a directory traversal vulnerability. This could allow context-dependent attackers to write arbitrary files via a specially crafted ZIP file. (CVE-2008-5658)

Certain versions of PHP ship with a flawed implementation of magic_quotes_gpc. This could allow context-dependent attackers to conduct SQL injection attacks. (CVE-2008-5844)

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	30087
BID	31681
BID	30649
BID	32948
BID	32688
BID	32383
BID	32625
CVE	CVE-2008-2371
CVE	CVE-2008-3658
CVE	CVE-2008-3659
CVE	CVE-2008-3660
CVE	CVE-2008-5557
CVE	CVE-2008-5624
CVE	CVE-2008-5625
CVE	CVE-2008-5658
CVE	CVE-2008-5844

Source	Reference
SECUNIA	32964
URL	http://www.php.net/ChangeLog-5.php#5.2.8
URL	http://bugs.php.net/bug.php?id=45722
URL	http://bugs.php.net/bug.php?id=42718

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.2.8.tar.gz/from/a/mirror
Upgrade to PHP v5.2.8 (released on December 8th, 2008).

3.1.5. PHP 5.2.5 cURL safe_mode bypass (http-php-curl-safe-mode-bypass-other)

Description:

Certain versions of PHP contain a weakness whereby calls to the cURL extension can bypass Safe Mode restrictions. As a result, a script can be constructed to access files it did not normally have permission to manipulate.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
CVE	CVE-2007-4850
BID	27413
SECUNIA	30048
URL	http://www.php.net/releases/5_2_6.php
URL	http://article.gmane.org/gmane.comp.security.full-disclosure/58593

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.2.6.tar.gz/from/a/mirror
Upgrade to PHP v5.2.6 (released on May 1st, 2008).

3.1.6. PHP Multiple Vulnerabilities Fixed in version 5.2.11 (http-php-multiple-vulns-5-2-11)

Description:

Fixed certificate validation inside php_openssl_apply_verification_policy (CVE-2009-3291)

Added missing sanity checks around exif processing (CVE-2009-3292)

Fixed sanity check for the color index in imagecolortransparent (CVE-2009-3293)

Fixed bug #44683 (popen crashes when an invalid mode is passed)

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
SECUNIA	36791
SECUNIA	37151
SECUNIA	37313
SECUNIA	37498
SECUNIA	38090
SECUNIA	38188
SECUNIA	40262
XF	php-certificate-unspecified(53334)
CVE	CVE-2009-3291
CVE	CVE-2009-3292
CVE	CVE-2009-3293
BID	36449
URL	http://www.php.net/releases/5_2_11.php
URL	http://www.php.net/ChangeLog-5.php#5.2.11
URL	http://bugs.php.net/44683

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.2.11.tar.gz/from/a/mirror
Upgrade to PHP v5.2.11 (released on September 16th, 2009).

3.1.7. PHP Multiple Vulnerabilities Fixed in version 5.2.12 (http-php-multiple-vulns-5-2-12)

Description:

Fixed a safe_mode bypass in tempnam() identified by Grzegorz Stachowiak (CVE-2009-3557)

Fixed a open_basedir bypass in posix_mkfifo() identified by Grzegorz Stachowiak (CVE-2009-3558)

Added "max_file_uploads" INI directive, which can be set to limit the number of file uploads per-request to 20 by default, to prevent possible DOS via temporary file exhaustion (CVE-2009-4017)

Added protection for $_SESSION from interrupt corruption and improved "session.save_path" check, identified by Stefan Esser (CVE-2009-4143)

Fixed bug #49785 (insufficient input string validation of htmlspecialchars()) (CVE-2009-4142)

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	37390
SECUNIA	37821
SECUNIA	38648
SECUNIA	40262
CVE	CVE-2009-3557
CVE	CVE-2009-3558
CVE	CVE-2009-4017
CVE	CVE-2009-4142
CVE	CVE-2009-4143
URL	http://www.php.net/releases/5_2_12.php

Source	Reference
URL	http://www.php.net/ChangeLog-5.php#5.2.12

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.2.12.tar.gz/from/a/mirror
Upgrade to PHP v5.2.12 (released on December 17th, 2009).

3.1.8. PHP Multiple Vulnerabilities Fixed in version 5.2.7 (http-php-multiple-vulns-5-2-7)

Description:

Heap-based buffer overflow in pcre_compile.c in the Perl-Compatible Regular Expression (PCRE) library 7.7 allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a regular expression that begins with an option and contains multiple branches. (CVE-2008-2371)

Directory traversal vulnerability in the posix_access function in PHP 5.2.6 and earlier allows remote attackers to bypass safe_mode restrictions via a .. (dot dot) in an http URL, which results in the URL being canonicalized to a local filename after the safe_mode check has successfully run. (CVE-2008-2665)

Multiple directory traversal vulnerabilities in PHP 5.2.6 and earlier allow context-dependent attackers to bypass safe_mode restrictions by creating a subdirectory named http: and then placing ../ (dot dot slash) sequences in an http URL argument to the (1) chdir or (2) ftok function. (CVE-2008-2666)

php_imap.c in PHP 5.2.5, 5.2.6, 4.x, and other versions, uses obsolete API calls that allow context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long IMAP request, which triggers an "rfc822.c legacy routine buffer overflow" error message, related to the rfc822_write_address function. (CVE-2008-2829)

Buffer overflow in the imageloadfont function in ext/gd/gd.c in PHP 4.4.x before 4.4.9 and PHP 5.2 before 5.2.6-r6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted font file. (CVE-2008-3658)

Buffer overflow in the memnstr function in PHP 4.4.x before 4.4.9 and PHP 5.2 through 5.2.6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via the delimiter argument to the explode function. NOTE: the scope of this issue is limited since most applications would not use an attacker-controlled delimiter, but local attacks against safe_mode are feasible. (CVE-2008-3659)

PHP 4.4.x before 4.4.9, and 5.x through 5.2.6, when used as a FastCGI module, allows remote attackers to cause a denial of service (crash) via a request with multiple dots preceding the extension, as demonstrated using foo..php. (CVE-2008-3660)

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	29796
BID	29797
BID	29829
BID	30649
BID	30087
CVE	CVE-2008-2371
CVE	CVE-2008-2665
CVE	CVE-2008-2666
CVE	CVE-2008-2829
CVE	CVE-2008-3658
CVE	CVE-2008-3659
CVE	CVE-2008-3660
SECUNIA	35306
SECUNIA	35650
XF	php-chdir-ftoc-security-bypass(43198)
XF	php-curl-unspecified(44402)
XF	php-imageloadfont-dos(44401)
XF	php-memnstr-bo(44405)
XF	php-phpimap-dos(43357)
XF	php-posixaccess-security-bypass(43196)
URL	http://www.php.net/releases/5_2_7.php
URL	http://www.php.net/ChangeLog-5.php#5.2.7

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.2.7.tar.gz/from/a/mirror

Upgrade to PHP v5.2.7 (released on December 4th, 2008).

3.1.9. PHP "safe_mode" Multiple Security Bypass (http-php-safemode-bypass3)

Description:

Certain versions of PHP contain an implementation flaw in the 'posix_access()' function that allows remote attackers bypass safe_mode restrictions.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
CVE	CVE-2008-2665
CVE	CVE-2008-2666
BID	29796
BID	29797
URL	http://www.php.net/ChangeLog-5.php#5.2.8

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.2.8.tar.gz/from/a/mirror

Upgrade to PHP v5.2.8 (released on December 8th, 2008).

3.2. Severe Vulnerabilities

3.2.1. Apache APR-util XML Denial of Service (http-apache-apr-util-xml-dos)

Description:

A denial of service flaw was found in the bundled copy of the APR-util library Extensible Markup Language (XML) parser. A remote attacker could create a specially-crafted XML document that would cause excessive memory consumption when processed by the XML decoding engine.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	35253
CVE	CVE-2009-1955
SECUNIA	35284
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.bz2

Many platforms and distributions provide pre-built binary packages for Apache. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.2. Apache mod_prixy_ftp FTP Command Injection (http-apache-mod_proxy_ftp-command-injection)

Description:

A flaw was found in the mod_proxy_ftp module. In a reverse proxy configuration, a remote attacker could use this flaw to bypass intended access restrictions by creating a carefully-crafted HTTP Authorization header, allowing the attacker to send arbitrary commands to the FTP server.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	36254
CVE	CVE-2007-6422
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.14.tar.bz2

Many platforms and distributions provide pre-built binary packages for Apache. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating

system.

3.2.3. Apache APR-util Off-by-one Overflow (http-apache-apr-util-off-by-one-overflow)

Description:

An off-by-one overflow flaw was found in the way the bundled copy of the APR-util library processed a variable list of arguments. An attacker could provide a specially-crafted string as input for the formatted output conversion routine, which could, on big-endian platforms, potentially lead to the disclosure of sensitive information or a denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	35251
CVE	CVE-2009-1956
SECUNIA	35284
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.bz2

Many platforms and distributions provide pre-built binary packages for Apache. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.4. PHP Multiple Vulnerabilities Fixed in version 5.2.10 (http-php-multiple-vulns-5-2-10)

Description:

PHP versions before 5.2.10 can segfault on certain corrupted jpeg files in exit_read_data().

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
CVE	CVE-2009-2687
URL	http://www.php.net/releases/5_2_10.php
URL	http://www.php.net/ChangeLog-5.php#5.2.10

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.2.10.tar.gz/from/a/mirror

Upgrade to PHP v5.2.10 (released on June 18th, 2009).

3.2.5. PHP Multiple Vulnerabilities Fixed in version 5.2.13 (http-php-multiple-vulns-5-2-13)

Description:

Improved LCG entropy (CVE-2010-1128)

Fixed safe_mode validation inside tempnam() when the directory path does not end with a / (CVE-2010-1129)

Fixed a possible open_basedir/safe_mode bypass in the session extension identified by Grzegorz Stachowiak (CVE-2010-1130)

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
CVE	CVE-2010-1128
CVE	CVE-2010-1129
CVE	CVE-2010-1130
URL	http://www.php.net/releases/5_2_13.php
URL	http://www.php.net/ChangeLog-5.php#5.2.13

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.2.13.tar.gz/from/a/mirror
Upgrade to PHP v5.2.13 (released on February 25th, 2010).

3.2.6. PHP Multiple Vulnerabilities Fixed in version 5.2.9 (http-php-multiple-vulns-5-2-9)

Description:

Certain versions of PHP ship with a vulnerable version of the imageRotate function. This could allow a context-dependent attacker to read the contents of arbitrary memory via a specially crafted value of the third argument for an indexed image. (CVE-2008-5498)

An unspecified error in the zip functionality could cause a crash when file or directory names contain a relative path (CVE-2009-1272)

An unspecified error exists in the explode() function.

An unspecified error exists when a malformed string is passed to the json_decode() function (CVE-2009-1271)

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	33002
CVE	CVE-2008-5498
CVE	CVE-2009-1271
CVE	CVE-2009-1272
SECUNIA	34081
URL	http://www.php.net/releases/5_2_9.php
URL	http://www.php.net/ChangeLog-5.php#5.2.9

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.2.9.tar.gz/from/a/mirror
Upgrade to PHP v5.2.9 (released on February 26th, 2009).

3.2.7. PHP Multiple Vulnerabilities Fixed in version 5.3.1 (http-php-multiple-vulns-5-3-1)

Description:

Added "max_file_uploads" INI directive, which can be set to limit the number of file uploads per-request to 20 by default, to prevent possible DOS via temporary file exhaustion.

Added missing sanity checks around exif processing.

Fixed a safe_mode bypass in tempnam().

Fixed a open_basedir bypass in posix_mkfifo().

Fixed bug #50063 (safe_mode_include_dir fails).

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
CVE	CVE-2009-3292
CVE	CVE-2009-3557
CVE	CVE-2009-3558
CVE	CVE-2009-3559
CVE	CVE-2009-4017
URL	http://www.php.net/releases/5_3_1.php
URL	http://www.php.net/ChangeLog-5.php#5.3.1

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.3.1.tar.gz/from/a/mirror
Upgrade to PHP v5.3.1 (released on November 19th, 2009).

3.2.8. PHP Multiple Vulnerabilities Fixed in version 5.3.2 (http-php-multiple-vulns-5-3-2)

Description:

Improved LCG entropy.

Fixed safe_mode validation inside tempnam() when the directory path does not end with a /.

Fixed a possible open_basedir/safe_mode bypass in the session extension identified by Grzegorz Stachowiak.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
URL	http://www.php.net/releases/5_3_2.php
URL	http://www.php.net/ChangeLog-5.php#5.3.2

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.3.2.tar.gz/from/a/mirror
Upgrade to PHP v5.3.2 (released on March 4th, 2010).

3.2.9. PHP rfc822_write_address Function Buffer Overflow (http-php-rfc822-write-address-bof)

Description:

Buffer overflow in PHP before 5.2.8 allows remote attackers to execute arbitrary code via a long IMAP request.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
CVE	CVE-2008-2829
BID	29829

Source	Reference
SECUNIA	32964
URL	http://www.php.net/ChangeLog-5.php#5.2.8
URL	http://bugs.php.net/bug.php?id=42862

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.2.8.tar.gz/from/a/mirror
Upgrade to PHP v5.2.8 (released on December 8th, 2008).

3.2.10. phpMyAdmin SQL Injection Vulnerability (Delayed Cross Site Request Forgery) (phpmyadmin-pmasa-2008-1)

Description:

Certain versions of phpMyAdmin access $_REQUEST to obtain some parameters instead of $_GET and $_POST. This could allow attackers, within the same domain, to override certain variables and conduct SQL injection and cross site request forgery attacks by using crafted cookies.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247 (209-20-76-247.slicehost.net)	Vulnerable software installed: phpMyAdmin 2.11.3

References:

Source	Reference
BID	28068
CVE	CVE-2008-1149
SECUNIA	29200
URL	http://www.phpmyadmin.net/home_page/security/PMASA-2008-1.php

Vulnerability Solution:

Download and apply the upgrade from: http://prdownloads.sourceforge.net/phpmyadmin/phpMyAdmin-2.11.5-english.tar.bz2?download

3.2.11. phpMyAdmin File Disclosure on Shared Hosts Via a Crafted HTTP POST Request (phpmyadmin-pmasa-2008-3)

Description:

An unspecified vulnerability exists in versions of phpMyAdmin before 2.11.5.2. When running on shared hosts, this could allow remote authenticated users with CREATE table permissions to read arbitrary files via a crafted HTTP POST request, related to use of an undefined UploadDir variable.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247 (209-20-76-247.slicehost.net)	Vulnerable software installed: phpMyAdmin 2.11.3

References:

Source	Reference
BID	28906
CVE	CVE-2008-1924
SECUNIA	29944
URL	http://www.phpmyadmin.net/home_page/security/PMASA-2008-3.php

Vulnerability Solution:

Download and apply the upgrade from: http://prdownloads.sourceforge.net/phpmyadmin/phpMyAdmin-2.11.5.2-english.tar.bz2?download

3.2.12. phpMyAdmin XSS on Plausible Insecure PHP Installation (phpmyadmin-pmasa-2008-4)

Description:

A cross-site scripting (XSS) vulnerability exists in versions of phpMyAdmin before 2.11.7, when register_globals is enabled and .htaccess support is disabled. This could allow remote attackers to inject arbitrary web script or HTML via unspecified vectors involving scripts in libraries/.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247 (209-20-76-247.slicehost.net)	Vulnerable software installed: phpMyAdmin 2.11.3

References:

Source	Reference
CVE	CVE-2008-2960

Source	Reference
SECUNIA	30813
URL	http://www.phpmyadmin.net/home_page/security/PMASA-2008-4.php

Vulnerability Solution:

Download and apply the upgrade from: http://prdownloads.sourceforge.net/phpmyadmin/phpMyAdmin-2.11.7-english.tar.bz2?download

3.2.13. phpMyAdmin XSRF/CSRF for Creating a Database and Modifying User Charset (phpmyadmin-pmasa-2008-5)

Description:

A cross-site request forgery (CSRF) vulnerability exists in versions of phpMyAdmin before 2.11.7.1. This could allow remote attackers to perform unauthorized actions via a link or IMG tag to the db parameter in the "Creating a Database" functionality (db_create.php), and the convcharset and collation_connection parameters related to an unspecified program that modifies the connection character set.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247 (209-20-76-247.slicehost.net)	Vulnerable software installed: phpMyAdmin 2.11.3

References:

Source	Reference
CVE	CVE-2008-3197
SECUNIA	31115
URL	http://www.phpmyadmin.net/home_page/security/PMASA-2008-5.php

Vulnerability Solution:

Download and apply the upgrade from: http://prdownloads.sourceforge.net/phpmyadmin/phpMyAdmin-2.11.7.1-english.tar.bz2?download

3.2.14. phpMyAdmin Cross-site Framing; XSS in setup.php (phpmyadmin-pmasa-2008-6)

Description:

Versions of phpMyAdmin before 2.11.8 are vulnerable to the following:

• Affected versions do not sufficiently prevent its pages from using frames that point to pages in other domains. This could make it easier for remote attackers to conduct spoofing or phishing activities via a cross-site framing attack. (CVE-2008-3456)

• A cross-site scripting (XSS) vulnerability exists in setup.php. This could allow user-assisted remote attackers with the ability to modify config/config.inc.php to inject arbitrary web script or HTML via crafted setup arguments. (CVE-2008-3457)

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247 (209-20-76-247.slicehost.net)	Vulnerable software installed: phpMyAdmin 2.11.3

References:

Source	Reference
BID	30420
CVE	CVE-2008-3456
CVE	CVE-2008-3457
SECUNIA	31263
URL	http://www.phpmyadmin.net/home_page/security/PMASA-2008-6.php

Vulnerability Solution:

Download and apply the upgrade from: http://prdownloads.sourceforge.net/phpmyadmin/phpMyAdmin-2.11.8-english.tar.bz2?download

3.2.15. X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch)

Description:

The subject common name (CN) field in the X.509 certificate does not match the name of the entity presenting the certificate.

Before issuing a certificate, a Certification Authority (CA) must check the identity of the entity requesting the certificate, as specified in the CA's Certification Practice Statement (CPS). Thus, standard certificate validation procedures require the subject CN field of a certificate to match the actual name of the entity presenting the certificate. For example, in a certificate presented by "https://www.example.com/", the CN should be "www.example.com".

In order to detect and prevent active eavesdropping attacks, the validity of a certificate must be verified, else an attacker could then launch a man-in-the-middle attack and gain full control of the data stream. Of particular importance is the validity of the subject's CN, that should match the name of the entity (hostname).

A CN mismatch most often occurs due to a configuration error, though it can also indicate that a man-in-the-middle attack is being conducted.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:25 (209-20-76-247.slicehost.net)	The subject common name found in the X.509 certificate ('CN=westsystem') does not seem to match the scan target 'westsystem.com':Subject CN 'westsystem' does not match node name 'westsystem.com'Subject CN 'westsystem' does not match DNS name '209.20.76.247'

References:

None

Vulnerability Solution:

The subject's common name (CN) field in the X.509 certificate should be fixed to reflect the name of the entity presenting the certificate (e.g., the hostname). This is done by generating a new certificate usually signed by a Certification Authority (CA) trusted by both the client and server.

3.2.16. Apache AllowOverride Options handling bypass (http-apache-allowoveride-options-handling-bypass)

Description:

A flaw was found in the handling of the "Options" and "AllowOverride" directives. In configurations using the "AllowOverride" directive with certain "Options=" arguments, local users were not restricted from executing commands from a Server-Side-Include script as intended.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	35115
CVE	CVE-2009-1195
SECUNIA	35261
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.bz2

Many platforms and distributions provide pre-built binary packages for Apache. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.17. Apache mod_proxy Reverse Proxy Denial of Service (http-apache-mod_proxy-reverse-proxy-dos)

Description:

A denial of service flaw was found in the mod_proxy module when it was used as a reverse proxy. A remote attacker could use this flaw to force a proxy process to consume large amounts of CPU time.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	35565
CVE	CVE-2009-1890
SECUNIA	35691
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.bz2

Many platforms and distributions provide pre-built binary packages for Apache. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.18. Apache mod_proxy_ajp Denial of Service (http-apache-mod_proxy_ajp-dos)

Description:

mod_proxy_ajp would return the wrong status code if it encountered an error, causing a backend server to be put into an error state until the retry timeout expired. A remote attacker could send malicious requests to trigger this issue, resulting in denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	38491
CVE	CVE-2010-0408
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.bz2

Many platforms and distributions provide pre-built binary packages for Apache. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.19. Apache mod_proxy_ftp Denial of Service (http-apache-mod_proxy_ftp-dos)

Description:

A NULL pointer dereference flaw was found in the mod_proxy_ftp module. A malicious FTP server to which requests are being proxied could use this flaw to crash an httpd child process via a malformed reply to the EPSV or PASV commands, resulting in a limited denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	36260
CVE	CVE-2009-3094
SECUNIA	36549
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.14.tar.bz2

Many platforms and distributions provide pre-built binary packages for Apache. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating

system.

3.2.20. Browsable web directory (http-generic-browsable-dir)

Description:

A web directory was found to be browsable, which means that anyone can see the contents of the directory. These directories can be found:

•via page spidering (following hyperlinks), or
•as part of a parent path (checking each directory along the path and searching for "Directory Listing" or similar strings), or
•by brute forcing a list of common directories.

Browsable directories could allow an attacker to view "hidden" files in the web root, including CGI scripts, data files, or backup pages.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	http://westsystem.com/css/blueprint/src/ 5: </head> 6: <body> 7: Index of /css/blueprint/src 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><t...
209.20.76.247:80 (209-20-76-247.slicehost.net)	http://westsystem.com/css/ 5: </head> 6: <body> 7: Index of /css 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> </td><...
209.20.76.247:80 (209-20-76-247.slicehost.net)	http://westsystem.com/css/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 5: </head> 6: <body> 7: Index of /css 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> </td><...

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	http://westsystem.com/css/blueprint/ 5: </head> 6: <body> 7: Index of /css/blueprint 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> </...
209.20.76.247:80 (209-20-76-247.slicehost.net)	http://westsystem.com/css/blueprint/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 5: </head> 6: <body> 7: Index of /css/blueprint 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> </...
209.20.76.247:80 (209-20-76-247.slicehost.net)	http://westsystem.com/css/blueprint/plugins/ 5: </head> 6: <body> 7: Index of /css/blueprint/plugins 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><t...
209.20.76.247:80 (209-20-76-247.slicehost.net)	http://westsystem.com/css/blueprint/plugins/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 5: </head> 6: <body> 7: Index of /css/blueprint/plugins 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><t...
209.20.76.247:80 (209-20-76-247.slicehost.net)	http://westsystem.com/css/blueprint/plugins/fancy-type/ 5: </head> 6: <body> 7: Index of /css/blueprint/plugins/fancy-type 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td><a href="/css/blueprint/plugins/">Parent Directory</a...
209.20.76.247:80 (209-20-76-247.slicehost.net)	http://westsystem.com/css/blueprint/plugins/fancy-type/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-

Affected Nodes:	Additional Information:
	5: </head> 6: <body> 7: Index of /css/blueprint/plugins/fancy-type 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td><a href="/css/blueprint/plugins/">Parent Directory</a...
209.20.76.247:80 (209-20-76-247.slicehost.net)	http://westsystem.com/css/blueprint/src/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 5: </head> 6: <body> 7: Index of /css/blueprint/src 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><t...
209.20.76.247:80 (209-20-76-247.slicehost.net)	http://westsystem.com/icons/ 5: </head> 6: <body> 7: Index of /icons 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> </td><...
209.20.76.247:80 (209-20-76-247.slicehost.net)	http://westsystem.com/icons/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 5: </head> 6: <body> 7: Index of /icons 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> </td><...
209.20.76.247:80 (209-20-76-247.slicehost.net)	http://westsystem.com/icons/small/ 5: </head> 6: <body> 7: Index of /icons/small 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> ...
209.20.76.247:80 (209-20-76-247.slicehost.net)	http://westsystem.com/icons/small/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 5: </head> 6: <body> 7: Index of /icons/small

Affected Nodes:	Additional Information:
	8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> ...
209.20.76.247:80 (209-20-76-247.slicehost.net)	http://westsystem.com/images/ 5: </head> 6: <body> 7: Index of /images 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> </td><...
209.20.76.247:80 (209-20-76-247.slicehost.net)	http://westsystem.com/images/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 5: </head> 6: <body> 7: Index of /images 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> </td><...
209.20.76.247:80 (209-20-76-247.slicehost.net)	http://westsystem.com/images/ps/ 5: </head> 6: <body> 7: Index of /images/ps 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> ...
209.20.76.247:80 (209-20-76-247.slicehost.net)	http://westsystem.com/images/ps/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 5: </head> 6: <body> 7: Index of /images/ps 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> ...
209.20.76.247:80 (209-20-76-247.slicehost.net)	http://westsystem.com/js/ 5: </head> 6: <body> 7: Index of /js 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> </td><...

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	http://westsystem.com/js/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 5: </head> 6: <body> 7: Index of /js 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> </td><...

References:

None

Vulnerability Solution:

•Apache

Disable web directory browsing for all directories and subdirectories

In your httpd.conf file, disable the "Indexes" option for the appropriate <Directory> tag by removing it from the Options line.

In addition, you should always make sure that proper permissions are set on all files and directories within the web root (including CGI scripts and backup files). Do not copy files in the web root unless you want these files to be available over the web. Periodically go through your web directories and clean out any unused, obsolete, or unknown files and directories.

•IIS, PWS, Microsoft-IIS, Internet Information Server, Internet Information Services, Microsoft-PWS

Disable web directory browsing for all directories and subdirectories

In the Internet Information Services control panel or MMC, choose the appropriate virtual directory entry and select Properties. Uncheck the 'Allow Directory Browsing' option.

In addition, you should always make sure that proper permissions are set on all files and directories within the web root (including CGI scripts and backup files). Do not copy files in the web root unless you want these files to be available over the web. Periodically go through your web directories and clean out any unused, obsolete, or unknown files and directories.

•Java System Web Server, iPlanet

Disable web directory indexing for all directories and subdirectories

The iPlanet web server indexes directories by searching the directory for an index file (by default index.html or home.html). If an index file is not found, the Document Preferences settings are checked to see what the Directory Indexing setting contains. This should be set to None to disable directory indexing.

For older versions of iPlanet that do not support the Directory Indexing setting, create a file called index.html or home.html in each directory. This page will then be served instead of a directory listing.

•Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote

Disable web directory browsing for all directories and subdirectories

Edit Tomcat's web.xml file. In the "default" servlet, change the "listings" parameter from "true" to "false". Restart the server.

In addition, you should always make sure that proper permissions are set on all files and directories within the web root (including CGI

scripts and backup files). Do not copy files in the web root unless you want these files to be available over the web. Periodically go through your web directories and clean out any unused, obsolete, or unknown files and directories.

3.2.21. PHP Multiple Vulnerabilities Fixed in version 5.2.5 (http-php-multiple-vulns-5-2-5)

Description:

Various iconv_*() functions allow context-dependent attackers to cause a denial of service (application crash) via a long arguments (CVE-2007-4840, CVE-2007-4783).

The dl() function allows context-dependent attackers to cause a denial of service (application crash) via a long string in the library parameter. (CVE-2007-4887).

htmlentities/htmlspecialchars accept partial multibyte sequences (CVE-2007-5898).

The automatic session id insertion feature in output_add_rewrite_var() adds the session id to non-local forms (CVE-2007-5899).

Values set with php_admin_* in httpd.conf can be overwritten with ini_set() (CVE-2007-5900).

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	26403
CVE	CVE-2007-4783
CVE	CVE-2007-4840
CVE	CVE-2007-4887
CVE	CVE-2007-5898
CVE	CVE-2007-5899
CVE	CVE-2007-5900
SECUNIA	27648
URL	http://www.php.net/releases/5_2_5.php

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.2.5.tar.gz/from/a/mirror
Upgrade to PHP v5.2.5 (released on November 8, 2007).

3.2.22. Apache APR-util Heap Underwrite (http-apache-apr-util-heap-underwrite)

Description:

A heap-based underwrite flaw was found in the way the bundled copy of the APR-util library created compiled forms of particular search patterns. An attacker could formulate a specially-crafted search keyword, that would overwrite arbitrary heap memory locations when processed by the pattern preparation engine.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	35221
CVE	CVE-2009-0023
SECUNIA	35284
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3
Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.bz2
Many platforms and distributions provide pre-built binary packages for Apache. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.23. Apache mod_deflate Denial of Service (http-apache-mod_deflate-dos)

Description:

A denial of service flaw was found in the mod_deflate module. This module continued to compress large files until compression was complete, even if the network connection that requested the content was closed before compression completed. This would cause mod_deflate to consume large amounts of CPU if mod_deflate was enabled for a large file.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	35623
CVE	CVE-2009-1891
SECUNIA	35781
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.bz2

Many platforms and distributions provide pre-built binary packages for Apache. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.24. Apache Request Header Information Disclosure (http-apache-request-header-info-disclosure)

Description:

A flaw in the core subrequest process code was fixed, to always provide a shallow copy of the headers_in array to the subrequest, instead of a pointer to the parent request's array as it had for requests without request bodies. This meant all modules such as mod_headers which may manipulate the input headers for a subrequest would poison the parent request in two ways, one by modifying the parent request, which might not be intended, and second by leaving pointers to modified header fields in memory allocated to the subrequest scope, which could be freed before the main request processing was finished, resulting in a segfault or in revealing data from another request on threaded servers, such as the worker or winnt MPMs.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	38494
CVE	CVE-2010-0434
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3
Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.bz2
Many platforms and distributions provide pre-built binary packages for Apache. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.25. phpMyAdmin Credentials Disclosure on Shared Hosts Via Session Data (phpmyadmin-pmasa-2008-2)

Description:

Versions of phpMyAdmin before 2.11.5.1 store the MySQL username, password, and the Blowfish secret key in cleartext in a Session file under /tmp. This could allow local users to obtain sensitive information.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247 (209-20-76-247.slicehost.net)	Vulnerable software installed: phpMyAdmin 2.11.3

References:

Source	Reference
BID	28560
CVE	CVE-2008-1567
SECUNIA	29613
URL	http://www.phpmyadmin.net/home_page/security/PMASA-2008-2.php

Vulnerability Solution:

Download and apply the upgrade from: http://prdownloads.sourceforge.net/phpmyadmin/phpMyAdmin-2.11.5.1-english.tar.bz2?download

3.2.26. Self-signed TLS/SSL certificate (ssl-self-signed-certificate)

Description:

The server's TLS/SSL certificate is self-signed. Self-signed certificates cannot be trusted by default, especially because TLS/SSL man-in-the-middle attacks typically use self-signed certificates to eavesdrop on TLS/SSL connections.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:25 (209-20-76-247.slicehost.net)	TLS/SSL certificate is self-signed.

References:

None

Vulnerability Solution:

Obtain a new TLS/SSL server certificate that is NOT self-signed and install it on the server. The exact instructions for obtaining a new certificate depend on your organization's requirements. Generally, you will need to generate a certificate request and save the request as a file. This file is then sent to a Certificate Authority (CA) for processing. Your organization may have its own internal Certificate Authority. If not, you may have to pay for a certificate from a trusted external Certificate Authority, such as Thawte or Verisign.

3.3. Moderate Vulnerabilities

3.3.1. HTTP TRACE Method Enabled (http-trace-method-enabled)

Description:

The HTTP TRACE method is normally used to return the full HTTP request back to the requesting client for proxy-debugging purposes. An attacker can create a webpage using XMLHTTP, ActiveX, or XMLDOM to cause a client to issue a TRACE request and capture the client's cookies. This effectively results in a Cross-Site Scripting attack.

Affected Nodes:

Affected Nodes:	Additional Information:

209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service.
	http://westsystem.com/
	`1: TRACE / HTTP/1.1`
	`2: Host: westsystem.com`
	`3: Cookie:` vulnerable=yes

References:

Source	Reference
OSVDB	877
SUN	50603
URL	http://www.kb.cert.org/vuls/id/867593
BID	9561
URL	http://www.apacheweek.com/issues/03-01-24#news

Vulnerability Solution:

•Apache

Disable HTTP TRACE Method for Apache

Newer versions of Apache (1.3.34 and 2.0.55 and later) provide a configuration directive called TraceEnable. To deny TRACE requests, add the following line to the server configuration:

```
TraceEnable off
```

For older versions of the Apache webserver, use the mod_rewrite module to deny the TRACE requests:

```
RewriteEngine On
RewriteCond %{REQUEST_METHOD} ^TRACE
RewriteRule .* - [F]
```

•IIS, PWS, Microsoft-IIS, Internet Information Server, Internet Information Services, Microsoft-PWS

Disable HTTP TRACE Method for Microsoft IIS

For Microsoft Internet Information Services (IIS), you may use the URLScan tool, freely available at http://www.microsoft.com/technet/security/tools/urlscan.mspx

•Java System Web Server, SunONE WebServer, Sun-ONE-Web-Server, iPlanet

Disable HTTP TRACE Method for SunONE/iPlanet

•For Sun ONE/iPlanet Web Server v6.0 SP2 and later, add the following configuration to the top of the default object in the 'obj.conf' file:

```
<Client method="TRACE">
  AuthTrans fn="set-variable"
     remove-headers="transfer-encoding"
     set-headers="content-length: -1"
     error="501"
</Client>
```

You must then restart the server for the changes to take effect.

•For Sun ONE/iPlanet Web Server prior to v6.0 SP2, follow the instructions provided the 'Relief/Workaround' section of Sun's official advisory: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603

•Lotus Domino

Disable HTTP TRACE Method for Domino

Follow IBM's instructions for disabling HTTP methods on the Domino server by adding the following line to the server's NOTES.INI file:

```
HTTPDisableMethods=TRACE
```

After saving NOTES.INI, restart the Notes web server by issuing the console command "tell http restart".

3.3.2. WebDAV Extensions are Enabled (http-generic-webdav-enabled)

Description:

WebDAV is a set of extensions to the HTTP protocol that allows users to collaboratively edit and manage files on remote web servers. Many web servers enable WebDAV extensions by default, even when they are not needed. Because of its added complexity, it is considered good practice to disable WebDAV if it is not currently in use.

Affected Nodes:

Affected Nodes:	Additional Information:
209.20.76.247:80 (209-20-76-247.slicehost.net)	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
URL	http://www.nextgenss.com/papers/iisrconfig.pdf

Vulnerability Solution:

•IIS, PWS, Microsoft-IIS, Internet Information Server, Internet Information Services, Microsoft-PWS

Disable WebDAV for IIS

For Microsoft IIS, follow Microsoft's instructions to disable WebDAV for the entire server.

•Apache

Disable WebDAV for Apache

Make sure the mod_dav module is disabled, or ensure that authentication is required on directories where DAV is required.

•Apache Tomcat, Tomcat, Tomcat Web Server

Disable WebDAV for Apache Tomcat

Disable the WebDAV Servlet for all web applications found on the web server. This can be done by removing the servlet definition for WebDAV (the org.apache.catalina.servlets.WebdavServlet class) and remove all servlet mappings referring to the WebDAV servlet.

•Java System Web Server, iPlanet, SunONE WebServer, Sun-ONE-Web-Server

Disable WebDAV for iPlanet/Sun ONE

Disable WebDAV on the web server. This can be done by disabling WebDAV for the server instance and for all virtual servers.

To disable WebDAV for the server instance, enter the Server Manager and uncheck the "Enable WebDAV Globally" checkbox then click the "OK" button.

To disable WebDAV for each virtual server, enter the Class Manager and uncheck the "Enable WebDAV Globally" checkbox next to each server instance then click the "OK" button.

4. Discovered Services

4.1. HTTP

HTTP, the HyperText Transfer Protocol, is used to exchange multimedia content on the World Wide Web. The multimedia files commonly used with HTTP include text, sound, images and video.

4.1.1. General Security Issues

Simple authentication scheme

Many HTTP servers use BASIC as their primary mechanism for user authentication. This is a very simple scheme that uses base 64 to encode the cleartext user id and password. If a malicious user is in a position to monitor HTTP traffic, user ids and passwords can be stolen by decoding the base 64 authentication data. To secure the authentication process, use HTTPS (HTTP over TLS/SSL) connections to transmit the authentication data.

4.1.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
209.20.76.247 (209-20-76-247.slicehost.net)	tcp	80	8	•Apache 2.2.8 •PHP: 5.2.4-2ubuntu5.1 •WebDAV: •http.banner: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.1 with Suhosin-Patch •http.banner.server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.1 with Suhosin-Patch

4.2. SMTP

SMTP, the Simple Mail Transfer Protocol, is the Internet standard way to send e-mail messages between hosts. Clients typically submit outgoing e-mail to their SMTP server, which then forwards the message on through other SMTP servers until it reaches its final destination.

4.2.1. General Security Issues

Installed by default

By default, most UNIX workstations come installed with the sendmail (or equivalent) SMTP server to handle mail for the local host (e.g. the output of some cron jobs is sent to the root account via email). Check your workstations to see if sendmail is running, by telnetting to port 25/tcp. If sendmail is running, you will see something like this: $ telnet mybox 25 Trying 192.168.0.1... Connected to mybox. Escape character is '^]'. 220 mybox. ESMTP Sendmail 8.12.2/8.12.2; Thu, 9 May 2002 03:16:26 -0700 (PDT) If sendmail is running and you don't need it, then disable it via /etc/rc.conf or your operating system's equivalent startup configuration file. If you do need SMTP for the localhost, make sure that the server is only listening on the loopback interface (127.0.0.1) and is not reachable by other hosts. Also be sure to check port 587/tcp, which some versions of sendmail use for outgoing mail submissions.

Promiscuous relay

Perhaps the most common security issue with SMTP servers is servers which act as a "promiscuous relay", or "open relay". This describes servers which accept and relay mail from anywhere to anywhere. This setup allows unauthenticated 3rd parties (spammers) to use your mail server to send their spam to unwitting recipients. Promiscuous relay checks are performed on all discovered SMTP servers. See "smtp-general-openrelay" for more information on this vulnerability and how to fix it.

4.2.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
209.20.76.247 (209-20-76-247.slicehost.net)	tcp	25	2	•Postfix •advertise-esmtp: 1 •advertised-esmtp-extension-count: 8 •advertises-esmtp: TRUE •max-message-size: 10240000 •smtp.banner: 220 209-20-76-247.slicehost.net ESMTP Postfix (Ubuntu) •smtp.cert.issuer.dn: EMAILADDRESS=root@westsystem, CN=westsystem, OU=Office for Complication of Otherwise Simple Affairs, O=OCOSA, L=Everywhere, ST=There is no such thing outside US, C=XX •smtp.cert.key.alg.name: RSA •smtp.cert.not.valid.after: Sat, 29 Nov 2008 15:11:39 EST •smtp.cert.not.valid.before: Thu, 30 Oct 2008 16:11:39 EDT •smtp.cert.selfsigned: true •smtp.cert.serial.number: 13144616916633977758 •smtp.cert.sig.alg.name: SHA1withRSA •smtp.cert.subject.dn: EMAILADDRESS=root@westsystem, CN=westsystem, OU=Office for Complication of Otherwise Simple Affairs, O=OCOSA, L=Everywhere, ST=There is no such thing outside US, C=XX •smtp.cert.validsignature: true •supports-8bitmime: TRUE •supports-debug: FALSE •supports-dsn: TRUE •supports-enhancedstatuscodes: TRUE •supports-etrn: TRUE •supports-expand: FALSE •supports-pipelining: TRUE •supports-size: TRUE

Device	Protocol	Port	Vulnerabilities	Additional Information
				•supports-starttls: TRUE •supports-turn: FALSE •supports-verify: FALSE •supports-vrfy: TRUE

4.3. SSH

SSH, or Secure SHell, is designed to be a replacement for the aging Telnet protocol. It primarily adds encryption and data integrity to Telnet, but can also provide superior authentication mechanisms such as public key authentication.

4.3.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
209.20.76.247 (209-20-76-247.slicehost.net)	tcp	22	0	•OpenSSH 4.7p1 •ssh.banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1.2 •ssh.protocol.version: 2.0 •ssh.rsa.pubkey.fingerprint: E429AFB32EE45EFC11AC0D0D76B2573B

5. Discovered Users and Groups

No user or group information was discovered during the scan.

6. Discovered Databases

No database information was discovered during the scan.

7. Discovered Files and Directories

No file or directory information was discovered during the scan.

8. Policy Evaluations

No policy evaluations were performed.

9. Spidered Web Sites

9.1. http://209.20.76.247:80

9.1.1. Common Default URLs

The following URLs were guessed. They are often included with default web server or web server add-on installations.

Access Error (403)

- cgi-bin
- doc

Successful (200)

- css
- icons
- images
- js

9.1.2. Guessed URLs

The following URLs were guessed using various tricks based on the discovered web site content.

Access Error (403)

- cgi-bin
  - ?P=+ADw-script+AD4-alert(42)+ADw-
    - script+AD4-
    - script+AD4-
- doc
  - %3f.jsp
  - .svn
    - entries
  - ADw-script AD4-alert(42) ADw-
    - script AD4-
  - CVS
    - Entries
    - Root
  - DEADJOE
  - Trace.axd
  - WS_FTP.LOG
  - Web.sitemap
  - adojavas.inc

- adovbs.inc
- web.config

Redirect (301)

- ?P=+ADw-script+AD4-alert(42)+ADw-
  - script+AD4-
- css
  - blueprint
  - blueprint
    - plugins
    - plugins
      - fancy-type
    - src
- icons
  - small
- images
- images
  - ps

Successful (200)

- css
  - ?P=+ADw-script+AD4-alert(42)+ADw-
    - script+AD4-
    - script+AD4-
    - script+AD4-
    - script+AD4-
    - script+AD4-
    - script+AD4-
    - script+AD4-
    - script+AD4-
    - script+AD4-
    - script+AD4-
  - blueprint
    - plugins
      - fancy-type
    - src
- icons
  - small
- images
  - ps

•js

9.1.3. Linked URLs

The following URLs were found as links in the content of other web pages.

Redirect (301)

Successful (200)

•css
 •blueprint
  •ie.css
  •plugins
   •fancy-type
    •readme.txt
    •screen.css
  •print.css
  •screen.css
  •src
   •forms.css
   •grid.css
   •ie.css
   •print.css
   •reset.css
   •typography.css
 •ie.css
 •jquery.lightbox-0.5.css
 •main.css
 •reset.css
 •sIFR-print.css
 •sIFR-screen.css
 •thickbox.css
 •typography.css
•icons
 •README
 •README.html
 •small
•images
 •ps
•js
 •AC_RunActiveContent.js

- domtab.js
- effects.js
- flashembed.min.js
- jquery.js
- jquery.js-old
- jquery.lightbox-0.5.js
- jquery.lightbox-0.5.min.js
- jquery.lightbox.packed.js
- jquery.validate.min.js
- jtip.js
- lightbox.js
- prototype.js
- scriptaculous.js
- sifr-config.js
- suckerfish.js
- swfobject.js
- thickbox.js
- westsystem.js