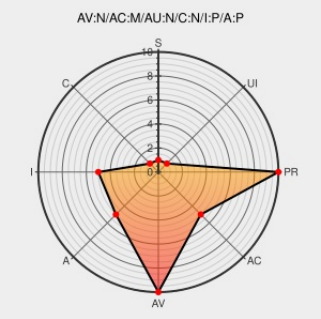
CVE-2012-1172

Published on: 05/23/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:18 PM UTC

CVE-2012-1172

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Php from Php contain the following vulnerability:

The file-upload implementation in rfc1867.c in PHP before 5.4.0 does not properly handle invalid [(open square bracket) characters in name values, which makes it easier for remote attackers to cause a denial of service (malformed $_FILES indexes) or conduct directory traversal attacks during multi-file uploads by leveraging a script that lacks its own filename restrictions.

CVE-2012-1172 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
PHP: Diff of /php/php-src/branches/PHP_5_4/main/rfc1867.c	Patch, svn.php.net, text/html	CONFIRM svn.php.net/viewvc/php/php-src/branches/PHP_5_4/main/rfc1867.c?r1=321664&r2=321663&pathrev=321664
APPLE-SA-2012-09-19-2 OS X Mountain Lion v10.8.2, OS X Lion v10.7.5 and Security Update 2012-004	lists.apple.com, text/html	APPLE APPLE-SA-2012-09-19-2
About the security content of OS X Mountain Lion v10.8.2, OS X Lion v10.7.5 and Security Update 2012-004	support.apple.com, text/html	CONFIRM support.apple.com/kb/HT5501
PHP :: Bug #48597 :: Unclosed array keys break space escaping in $_GET/POST/REQUEST	Exploit, bugs.php.net, text/xml	MISC bugs.php.net/bug.php?id=48597

[SECURITY] Fedora 15 Update: php-5.3.11-1.fc15	lists.fedoraproject.org text/html	FEDORA FEDORA-2012-6911
	Exploit students.mimuw.edu.pl application/pdf	MISC students.mimuw.edu.pl/~ai292615/php_multipleupload_overwrite.pdf
[SECURITY] Fedora 16 Update: php-5.3.11-1.fc16	lists.fedoraproject.org text/html	FEDORA FEDORA-2012-6907
oss-security - Re: CVE request for PHP 5.3.x Corrupted $_FILES indices lead to security concern	openwall.com text/html	MLIST [oss-security] 20120313 Re: CVE request for PHP 5.3.x Corrupted $_FILES indices lead to security concern
PHP :: Bug #49683 :: $_FILES overwrite	bugs.php.net text/xml	MISC bugs.php.net/bug.php?id=49683
[SECURITY] Fedora 17 Update: php-5.4.1-1.fc17	lists.fedoraproject.org text/html	FEDORA FEDORA-2012-6869
PHP: Revision 321664	svn.php.net text/html	CONFIRM svn.php.net/viewvc?view=revision&revision=321664
PHP: PHP 5 ChangeLog	www.php.net text/html	CONFIRM www.php.net/ChangeLog-5.php#5.4.0
Debian -- Security Information -- DSA-2465-1 php5	www.debian.org Depreciated Link text/html	DEBIAN DSA-2465
Directory Traversal via PHP Multi-File Uploads » Neal Poole	Exploit nealpoole.com text/html	MISC nealpoole.com/blog/2011/10/directory-traversal-via-php-multi-file-uploads/
PHP not properly checking Params | NYU Poly ISIS Lab	Exploit web.archive.org text/html Inactive Link Not Archived	MISC isisblogs.poly.edu/2011/08/11/php-not-properly-checking-params/
'[security bulletin] HPSBUX02791 SSRT100856 rev.1 - HP-UX Apache Web Server running PHP, Remote Execu' - MARC	marc.info text/html	HP SSRT100856
PHP :: Bug #54374 :: Insufficient validating of upload name leading to corrupted $_FILES indices	Exploit bugs.php.net text/xml	CONFIRM bugs.php.net/bug.php?id=54374
[security-announce] SUSE-SU-2012:0604-1: critical: Security update for P	lists.opensuse.org text/html	SUSE SUSE-SU-2012:0604
[security-announce] SUSE-SU-2012:0598-1: critical: Security update for P	lists.opensuse.org text/html	SUSE SUSE-SU-2012:0598
PHP :: You must be logged in	bugs.php.net text/xml	CONFIRM bugs.php.net/bug.php?id=55500

There are currently no OIDs associated with this CVE

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Php	Php	5.0.0	All	All	All
Application	Php	Php	5.0.0	beta1	All	All
Application	Php	Php	5.0.0	beta2	All	All
Application	Php	Php	5.0.0	beta3	All	All
Application	Php	Php	5.0.0	beta4	All	All
Application	Php	Php	5.0.0	rc1	All	All
Application	Php	Php	5.0.0	rc2	All	All
Application	Php	Php	5.0.0	rc3	All	All
Application	Php	Php	5.0.1	All	All	All
Application	Php	Php	5.0.2	All	All	All
Application	Php	Php	5.0.3	All	All	All
Application	Php	Php	5.0.4	All	All	All
Application	Php	Php	5.0.5	All	All	All
Application	Php	Php	5.1.0	All	All	All
Application	Php	Php	5.1.1	All	All	All
Application	Php	Php	5.1.2	All	All	All
Application	Php	Php	5.1.3	All	All	All
Application	Php	Php	5.1.4	All	All	All
Application	Php	Php	5.1.5	All	All	All
Application	Php	Php	5.1.6	All	All	All
Application	Php	Php	5.2.0	All	All	All
Application	Php	Php	5.2.1	All	All	All
Application	Php	Php	5.2.10	All	All	All
Application	Php	Php	5.2.11	All	All	All
Application	Php	Php	5.2.12	All	All	All
Application	Php	Php	5.2.13	All	All	All
Application	Php	Php	5.2.14	All	All	All
Application	Php	Php	5.2.15	All	All	All
Application	Php	Php	5.2.16	All	All	All
Application	Php	Php	5.2.17	All	All	All
Application	Php	Php	5.2.2	All	All	All
Application	Php	Php	5.2.3	All	All	All

Application	Php	Php	5.2.4	All	All	All
Application	Php	Php	5.2.5	All	All	All
Application	Php	Php	5.2.6	All	All	All
Application	Php	Php	5.2.7	All	All	All
Application	Php	Php	5.2.8	All	All	All
Application	Php	Php	5.2.9	All	All	All
Application	Php	Php	5.3.0	All	All	All
Application	Php	Php	5.3.1	All	All	All
Application	Php	Php	5.3.2	All	All	All
Application	Php	Php	5.3.3	All	All	All
Application	Php	Php	5.3.4	All	All	All
Application	Php	Php	5.3.5	All	All	All
Application	Php	Php	5.3.6	All	All	All
Application	Php	Php	5.3.7	All	All	All
Application	Php	Php	5.3.8	All	All	All
Application	Php	Php	5.3.9	All	All	All
Application	Php	Php	5.0.0	All	All	All
Application	Php	Php	5.0.0	beta1	All	All
Application	Php	Php	5.0.0	beta2	All	All
Application	Php	Php	5.0.0	beta3	All	All
Application	Php	Php	5.0.0	beta4	All	All
Application	Php	Php	5.0.0	rc1	All	All
Application	Php	Php	5.0.0	rc2	All	All
Application	Php	Php	5.0.0	rc3	All	All
Application	Php	Php	5.0.1	All	All	All
Application	Php	Php	5.0.2	All	All	All
Application	Php	Php	5.0.3	All	All	All
Application	Php	Php	5.0.4	All	All	All
Application	Php	Php	5.0.5	All	All	All
Application	Php	Php	5.1.0	All	All	All
Application	Php	Php	5.1.1	All	All	All
Application	Php	Php	5.1.2	All	All	All
Application	Php	Php	5.1.3	All	All	All
Application	Php	Php	5.1.4	All	All	All
Application	Php	Php	5.1.5	All	All	All
Application	Php	Php	5.1.6	All	All	All

Application	Php	Php	5.1.6	All	All	All
Application	Php	Php	5.2.0	All	All	All
Application	Php	Php	5.2.1	All	All	All
Application	Php	Php	5.2.10	All	All	All
Application	Php	Php	5.2.11	All	All	All
Application	Php	Php	5.2.12	All	All	All
Application	Php	Php	5.2.13	All	All	All
Application	Php	Php	5.2.14	All	All	All
Application	Php	Php	5.2.15	All	All	All
Application	Php	Php	5.2.16	All	All	All
Application	Php	Php	5.2.17	All	All	All
Application	Php	Php	5.2.2	All	All	All
Application	Php	Php	5.2.3	All	All	All
Application	Php	Php	5.2.4	All	All	All
Application	Php	Php	5.2.5	All	All	All
Application	Php	Php	5.2.6	All	All	All
Application	Php	Php	5.2.7	All	All	All
Application	Php	Php	5.2.8	All	All	All
Application	Php	Php	5.2.9	All	All	All
Application	Php	Php	5.3.0	All	All	All
Application	Php	Php	5.3.1	All	All	All
Application	Php	Php	5.3.2	All	All	All
Application	Php	Php	5.3.3	All	All	All
Application	Php	Php	5.3.4	All	All	All
Application	Php	Php	5.3.5	All	All	All
Application	Php	Php	5.3.6	All	All	All
Application	Php	Php	5.3.7	All	All	All
Application	Php	Php	5.3.8	All	All	All
Application	Php	Php	5.3.9	All	All	All
Application	Php	Php	All	All	All	All

cpe:2.3:a:php:php:5.0.0:*:*:*:*:*:*:*

cpe:2.3:a:php:php:5.0.0:beta1:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:beta2:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:beta3:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:beta4:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.1.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.10:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.11:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.12:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.13:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.14:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.15:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.16:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.17:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.7:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.8:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.9:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.7:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.8:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.9:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:beta1:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:beta2:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:beta3:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:beta4:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.1.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.10:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.11:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.12:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.13:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.14:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.15:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.16:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.17:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.7:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.8:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.9:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.7:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.8:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.9:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→