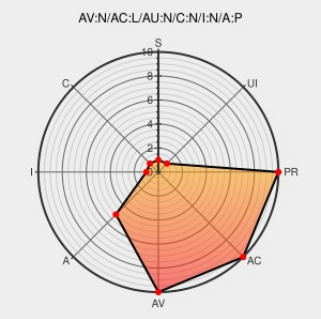
CVE-2009-4017

Published on: 11/23/2009 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:10:38 AM UTC

CVE-2009-4017

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



Certain versions of Php from Php contain the following vulnerability:

PHP before 5.2.12 and 5.3.x before 5.3.1 does not restrict the number of temporary files created when handling a multipart/form-data POST request, which allows remote attackers to cause a denial of service (resource exhaustion), and makes it easier for remote attackers to exploit local file inclusion vulnerabilities, via multiple requests, related to lack of support for the max_file_uploads directive.

CVE-2009-4017 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
PHP: PHP 5.2.12 Release Announcement	www.php.net text/html	CONFIRM www.php.net/releases/5_2_12.php
oss-security - Re: CVE request: php 5.3.1 update	www.openwall.com text/html	MLIST [oss-security] 20091120 Re: CVE request: php 5.3.1 update
HP System Management Homepage Multiple Vulnerabilities - Advisories - Community	web.archive.org text/html	SECUNIA 41480
'[security bulletin] HPSBUX02543 SSRT100152 rev.1 - HP-UX Running Apache with PHP, Remote Denial of S' - MARC	marc.info text/html	HP HPSBUX02543
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF php-multipart-formdata-dos(54455)

PHP: PHP 5.3.1 Release Announcement	Patch Vendor Advisory www.php.net text/html	CONFIRM www.php.net/releases/5_3_1.php
HP-UX update for Apache with PHP - Advisories - Community	web.archive.org text/html	SECUNIA 40262
PHP Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	SECUNIA 37821
No Description Provided	www.itrc.hp.com Inactive Link Not Archived	HP HPSBMA02568
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2009-3593
Support / Security / Advisories / / MDVSA-2009:305 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2009:305
Debian update for php5 - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	SECUNIA 37482
Acunetix Web Application Security Blog » PHP “multipart/form-data” denial of service	www.acunetix.com text/html	MISC www.acunetix.com/blog/websecuritynews/php-multipartform-data-denial-of-service/
APPLE-SA-2010-03-29-1 Security Update 2010-002 / Mac OS X v10.6.3	lists.apple.com text/html	APPLE APPLE-SA-2010-03-29-1
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20091120 PHP "multipart/form-data" denial of service
oss-security - CVE request: php 5.3.1 update	Patch www.openwall.com text/html	MLIST [oss-security] 20091120 CVE request: php 5.3.1 update
HP System Management Homepage Multiple Vulnerabilities - Advisories - Community	web.archive.org text/html	SECUNIA 41490
php.announce: 5.3.1 Release announcement	news.php.net text/xml	MLIST [php-announce] 20091119 5.3.1 Release announcement
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:10483
Debian -- Security Information -- DSA-1940-1 php5	www.debian.org Depreciated Link text/html	DEBIAN DSA-1940
Full Disclosure: PHP "multipart/form-data" denial of service	seclists.org text/html	FULLDISC 20091120 PHP "multipart/form-data" denial of service
PHP: PHP 5 ChangeLog	Patch Vendor Advisory www.php.net text/html	CONFIRM www.php.net/ChangeLog-5.php
About the security content of Security Update 2010-002 / Mac OS X v10.6.3	support.apple.com text/html	CONFIRM support.apple.com/kb/HT4077
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:6667
Support / Security / Advisories / / MDVSA-2009:303 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2009:303

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	5.2.11	All	All	All
Application	Php	Php	5.3.0	All	All	All
Application	Php	Php	5.2.11	All	All	All
Application	Php	Php	5.3.0	All	All	All

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

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→