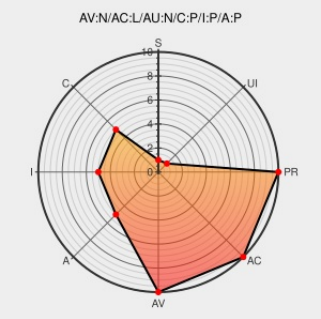
CVE-2007-4825

Published on: 09/11/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:32 PM UTC

CVE-2007-4825

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



Certain versions of Php from Php contain the following vulnerability:

Directory traversal vulnerability in PHP 5.2.4 and earlier allows attackers to bypass open_basedir restrictions and possibly execute arbitrary code via a .. (dot dot) in the dl function.

CVE-2007-4825 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
PHP: PHP 5 ChangeLog	www.php.net text/html	CONFIRM www.php.net/ChangeLog-5.php#5.2.5
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF php-dl-security-bypass(36528)
PHP 5.2.4 <= dl() extension_dir bypass&code exec&dos - CXSecurity.com	securityreason.com text/html	SREASON 3119
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 45902
Gentoo Linux Documentation -- PHP: Multiple vulnerabilities	www.gentoo.org text/html	GENTOO GLSA-200710-02
PHP: PHP 5.2.5 Release Announcement	www.php.net	CONFIRM www.php.net/releases/5_2_5.php

	text/html	
[security-announce] SUSE Security Announcement: php4, php5 (SUSE-SA:2008	lists.opensuse.org text/html	SUSE SUSE-SA:2008:004
SUSE update for php4 and php5 - Advisories - Secunia	web.archive.org text/html	SECUNIA 28658
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20070910 PHP <=5.2.4 open_basedir bypass & code exec & denial of service
Gentoo update for php - Advisories - Secunia	web.archive.org text/html	SECUNIA 27102
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20070910 /* PHP <=5.2.4 open_basedir bypass & code exec & denial of service errata ... working on windows too .. */
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20070910 Re: PHP <=5.2.4 open_basedir bypass & code exec & denial of service

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	All	All	All	All

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

← Previous ID

Next ID→

© CVE.report 2023 | |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report