

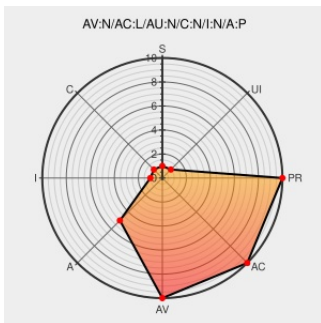


CVE-2009-1272

Published on: 04/08/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:27 PM UTC

CVE-2009-1272

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Php](#) from [Php](#) contain the following vulnerability:

The `php_zip_make_relative_path` function in `php_zip.c` in PHP 5.2.x before 5.2.9 allows context-dependent attackers to cause a denial of service (crash) via a ZIP file that contains filenames with relative paths, which is not properly handled during extraction.

CVE-2009-1272 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

oss-security - CVE request: PHP 5.2.9

[www.openwall.com](#)
[text/html](#)

[MLIST \[oss-security\] 20090401](#)
[CVE request: PHP 5.2.9](#)

About Security Update 2009-005

[support.apple.com](#)
[text/html](#)

[CONFIRM](#)
[support.apple.com/kb/HT3865](#)

PHP: PHP 5.2.9 Release Announcement

[Vendor Advisory](#)
[www.php.net](#)
[text/html](#)

[CONFIRM](#)
[www.php.net/releases/5_2_9.php](#)

No Description Provided

[cvs.php.net](#)
Inactive Link **Not Archived**

[MISC](#)
[cvs.php.net/viewvc.cgi/php-src/ext/zip/php_zip.c?r1=1.1.2.48&r2=1.1.2.49](#)

APPLE-SA-2009-09-10-2 Security Update 2009-005

[lists.apple.com](#)
[text/html](#)

[APPLE APPLE-SA-2009-09-10-2](#)

Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	 SECUNIA 36701
oss-security - Re: CVE request: PHP 5.2.9	www.openwall.com text/html	 MLIST [oss-security] 20090409 Re: CVE request: PHP 5.2.9
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	 SECUNIA 35685
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:012	lists.opensuse.org text/html	 SUSE SUSE-SR:2009:012
'[security bulletin] HPSBMA02447 SSRT090062 rev.1 - Insight Control Suite For Linux (ICE-LX) Cross Si' - MARC	marc.info text/html	 HP HPSBMA02447

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	5.2.0	All	All	All
Application	Php	Php	5.2.1	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	5.2.4	All	windows	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	5.2.0	All	All	All
Application	Php	Php	5.2.1	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	5.2.4	All	windows	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	CVE ID	CVSS	Severity	Exploitability
cpe:2.3:a:php:php:5.2.0:*:*:*:*:*:				
cpe:2.3:a:php:php:5.2.1:*:*:*:*:*:				
cpe:2.3:a:php:php:5.2.2:*:*:*:*:*:				
cpe:2.3:a:php:php:5.2.3:*:*:*:*:*:				
cpe:2.3:a:php:php:5.2.4:*:*:*:*:*:				
cpe:2.3:a:php:php:5.2.4*:windows:*:*:*:*:				
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:5.2.0:*:*:*:*:*:				
cpe:2.3:a:php:php:5.2.1:*:*:*:*:*:				
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:5.2.4*:windows:*:*:*:*:				
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:*:*:*:*:*:				

← Previous ID

Next ID →