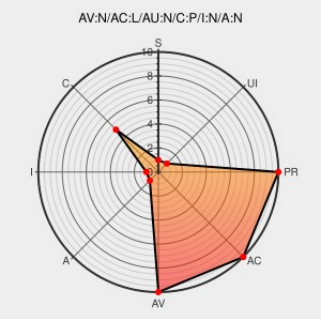
CVE-2010-2484

Published on: 08/20/2010 12:00:00 AM UTC

Last Modified on: 02/13/2023 03:06:56 AM UTC

CVE-2010-2484

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



Certain versions of Php from Php contain the following vulnerability:

The strrchr function in PHP 5.2 before 5.2.14 allows context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal function or handler.

CVE-2010-2484 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**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Bug 619324 – CVE-2010-2484 php: strrchr() interruption vulnerability	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=619324
APPLE-SA-2010-11-10-1 Mac OS X v10.6.5 and Security Update 2010-007	lists.apple.com text/html	APPLE APPLE-SA-2010-11-10-1
'[security bulletin] HPSBOV02763 SSRT100826 rev.1 - HP Secure Web Server (SWS) for OpenVMS running PH' - MARC	marc.info text/html	HP SSRT100826
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:018	lists.opensuse.org text/html	SUSE SUSE-SR:2010:018
APPLE-SA-2010-08-24-1 Security Update 2010-005	lists.apple.com text/html	APPLE APPLE-SA-2010-08-24-1
PHP: PHP 5.2.14 Release Announcement	www.php.net	CONFIRM

	text/html	www.php.net/releases/5_2_14.php
About Security Update 2010-005	support.apple.com text/html	CONFIRM support.apple.com/kb/HT4312
About the security content of Mac OS X v10.6.5 and Security Update 2010-007	web.archive.org text/html Inactive Link Not Archived	CONFIRM support.apple.com/kb/HT4435

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	5.2.10	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	5.2.2	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	5.2.8	All	All	All
Application	Php	Php	5.2.9	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	5.2.2	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	5.2.8	All	All	All
Application	Php	Php	5.2.9	All	All	All

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:5.2.2:*:*:*:*:*:*:*:

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:5.2.8:*:*:*:*:*:*:*:

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

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:5.2.2:*:*:*:*:*:*:*:

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:5.2.8:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→