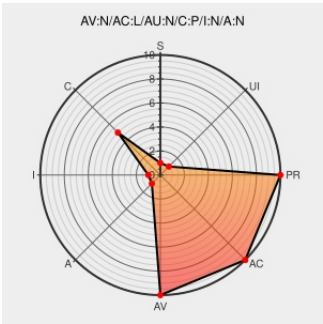
CVE-2004-1020

Published on: 12/08/2004 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:09 PM UTC

CVE-2004-1020

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



Certain versions of Php from Php contain the following vulnerability:

The addslashes function in PHP 4.3.9 does not properly escape a NULL (/0) character, which may allow remote attackers to read arbitrary files in PHP applications that contain a directory traversal vulnerability in require or include statements, but are otherwise protected by the magic_quotes_gpc mechanism. NOTE: this issue was originally REJECTed by its CNA before publication, but that decision is in active dispute. This candidate may change significantly in the future as a result of further discussion.

CVE-2004-1020 has been assigned by cve@mitre.org 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
Gentoo Linux Documentation -- PHP: Multiple vulnerabilities	Vendor Advisory, www.gentoo.org, text/html	GENTOO GLSA-200412-14
SecurityFocus	Exploit, Vendor Advisory, www.securityfocus.com, text/html	BUGTRAQ 20041216 PHP Input Validation Vulnerabilities
No Description Provided	web.archive.org, text/html, Inactive Link, Not Archived	HP HPSBMA01212

PHP Multiple Remote Vulnerabilities	Exploit Patch cve.report (archive) text/html	BID 11981
Advisories - Mandriva	www.mandriva.com text/html	MANDRAKE MDKSA-2004:151
PHP: PHP 4.3.10 Release Announcement	Vendor Advisory www.php.net text/html	CONFIRM www.php.net/release_4_3_10.php
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF php-addslashes-view-files(18516)
Home - Conectiva	distro.conectiva.com.br text/html	CONECTIVA CLA-2005:915

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	4.3.6	All	All	All
Application	Php	Php	4.3.7	All	All	All
Application	Php	Php	4.3.8	All	All	All
Application	Php	Php	4.3.9	All	All	All
Application	Php	Php	5.0	rc1	All	All
Application	Php	Php	5.0	rc2	All	All
Application	Php	Php	5.0	rc3	All	All
Application	Php	Php	5.0.0	All	All	All
Application	Php	Php	5.0.1	All	All	All
Application	Php	Php	5.0.2	All	All	All
Application	Php	Php	4.3.6	All	All	All
Application	Php	Php	4.3.7	All	All	All
Application	Php	Php	4.3.8	All	All	All
Application	Php	Php	4.3.9	All	All	All
Application	Php	Php	5.0	rc1	All	All
Application	Php	Php	5.0	rc2	All	All
Application	Php	Php	5.0	rc3	All	All
Application	Php	Php	5.0.0	All	All	All

Application	Php	Php	5.0.1	All	All	All
Application	Php	Php	5.0.2	All	All	All

- cpe:2.3:a:php:php:4.3.6:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:4.3.7:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:4.3.8:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:4.3.9:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.0:rc1:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.0:rc2:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.0:rc3:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.0.0:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.0.1:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.0.2:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:4.3.6:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:4.3.7:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:4.3.8:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:4.3.9:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.0:rc1:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.0:rc2:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.0:rc3:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.0.0:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.0.1:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.0.2:*:*:*:*:*:*:*:

← Previous ID

Next ID→

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