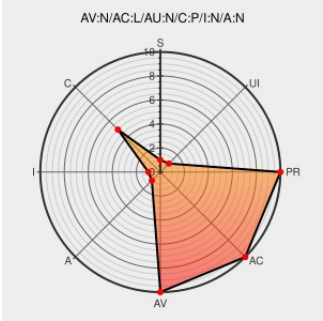
CVE-2006-4023

Published on: 08/08/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:57 PM UTC

CVE-2006-4023

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



Certain versions of Php from Php contain the following vulnerability:

The ip2long function in PHP 5.1.4 and earlier may incorrectly validate an arbitrary string and return a valid network IP address, which allows remote attackers to obtain network information and facilitate other attacks, as demonstrated using SQL injection in the X-FORWARDED-FOR Header in index.php in MiniBB 2.0. NOTE: it could be argued that the ip2long behavior represents a risk for security-relevant issues in a way that is similar to strcpy's role in buffer overflows, in which case this would be a class of implementation bugs that would require separate CVE items for each PHP application that uses ip2long in a security-relevant manner.

CVE-2006-4023 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
SecurityTracker.com Archives - PHP Error in ip2long() May Let Remote Users Inject SQL Commands Via Applications That Use the Function for Validation	Exploit, securitytracker.com, text/html	SECTRACK 1016609
Error 404 :(	Exploit, retrogod.altervista.org, text/plain, Inactive Link, Not Archived	MISC retrogod.altervista.org/php_ip2long.htm
SecurityFocus	www.securityfocus.com	BUGTRAQ 20060729 Re: PHP ip2long() function circumvention

	text/html	ip2long() function circumvention
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060729 PHP ip2long() function circumvention

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	4.3.3	All	All	All
Application	Php	Php	5.0.2	All	All	All
Application	Php	Php	5.1.4	All	All	All
Application	Php	Php	4.3.3	All	All	All
Application	Php	Php	5.0.2	All	All	All
Application	Php	Php	5.1.4	All	All	All

cpe:2.3:a:php:php:4.3.3:*:*:*:*:*:*:*

cpe:2.3:a:php:php:5.0.2:*:*:*:*:*:*:*

cpe:2.3:a:php:php:5.1.4:*:*:*:*:*:*:*

cpe:2.3:a:php:php:4.3.3:*:*:*:*:*:*:*

cpe:2.3:a:php:php:5.0.2:*:*:*:*:*:*:*

cpe:2.3:a:php:php:5.1.4:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→