



Published on: 04/26/2005 12:00:00 AM UTC

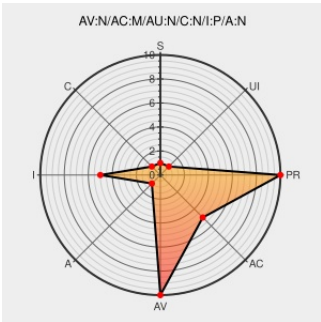
Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-1290

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

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

Multiple cross-site scripting (XSS) vulnerabilities in phpBB 2.0.14 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) u parameter to profile.php, (2) highlight parameter to viewtopic.php, or (3) forumname or forumdesc parameters to admin_forums.php.

CVE-2005-1290 has been assigned by [M cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
[N]eo [S]ecurity [T]eam	Exploit web.archive.org text/html Inactive Link Not Archived	🌐 MISC neosecurityteam.net/Advisories/Advisory-14.txt
No Description Provided	marc.info text/html	🌐 BUGTRAQ 20050423 ==phpBB 2.0.14 Multiple Vulnerabilities==

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	Phpbb Group	Phpbb	2.0.0	All	All	All
Application	Phpbb Group	Phpbb	2.0.1	All	All	All
Application	Phpbb Group	Phpbb	2.0.10	All	All	All
Application	Phpbb Group	Phpbb	2.0.11	All	All	All
Application	Phpbb Group	Phpbb	2.0.12	All	All	All
Application	Phpbb Group	Phpbb	2.0.13	All	All	All
Application	Phpbb Group	Phpbb	2.0.14	All	All	All
Application	Phpbb Group	Phpbb	2.0.2	All	All	All
Application	Phpbb Group	Phpbb	2.0.3	All	All	All
Application	Phpbb Group	Phpbb	2.0.4	All	All	All
Application	Phpbb Group	Phpbb	2.0.5	All	All	All
Application	Phpbb Group	Phpbb	2.0.6	All	All	All
Application	Phpbb Group	Phpbb	2.0.7	All	All	All
Application	Phpbb Group	Phpbb	2.0.8	All	All	All
Application	Phpbb Group	Phpbb	2.0.8a	All	All	All
Application	Phpbb Group	Phpbb	2.0.9	All	All	All
Application	Phpbb Group	Phpbb	2.0.0	All	All	All
Application	Phpbb Group	Phpbb	2.0.1	All	All	All
Application	Phpbb Group	Phpbb	2.0.10	All	All	All
Application	Phpbb Group	Phpbb	2.0.11	All	All	All
Application	Phpbb Group	Phpbb	2.0.12	All	All	All
Application	Phpbb Group	Phpbb	2.0.13	All	All	All
Application	Phpbb Group	Phpbb	2.0.14	All	All	All
Application	Phpbb Group	Phpbb	2.0.2	All	All	All
Application	Phpbb Group	Phpbb	2.0.3	All	All	All
Application	Phpbb Group	Phpbb	2.0.4	All	All	All
Application	Phpbb Group	Phpbb	2.0.5	All	All	All
Application	Phpbb Group	Phpbb	2.0.6	All	All	All
Application	Phpbb Group	Phpbb	2.0.7	All	All	All
Application	Phpbb Group	Phpbb	2.0.8	All	All	All
Application	Phpbb Group	Phpbb	2.0.8a	All	All	All
Application	Phpbb Group	Phpbb	2.0.9	All	All	All

Application	PHPBB Group	PHPBB	2.0.0	2.0.1	2.0.2	2.0.3
		cpe:2.3:a:phpbb_group:phpbb:2.0.0:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.1:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.10:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.11:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.12:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.13:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.14:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.2:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.3:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.4:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.5:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.6:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.7:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.8:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.8a:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.9:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.0:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.1:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.10:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.11:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.12:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.13:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.14:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.2:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.3:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.4:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.5:*****:				
		cpe:2.3:a:phpbb_group:phpbb:2.0.6:*****:				

cpe:2.3:a:phpbb_group:phpbb:2.0.7:*****:	
cpe:2.3:a:phpbb_group:phpbb:2.0.8:*****:	
cpe:2.3:a:phpbb_group:phpbb:2.0.8a:*****:	
cpe:2.3:a:phpbb_group:phpbb:2.0.9:*****:	
No vendor comments have been submitted for this CVE	
← 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 registered 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](#)