

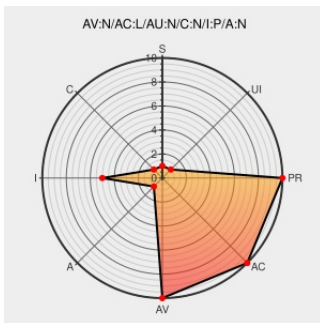


CVE-2004-2054

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:13 PM UTC

CVE-2004-2054

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

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

CRLF injection vulnerability in PhpBB 2.0.4 and 2.0.9 allows remote attackers to perform HTTP Response Splitting attacks to modify expected HTML content from the server via (1) the mode parameter to privmsg.php or (2) the redirect parameter to login.php.

CVE-2004-2054 has been assigned by [M](#) 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

NONE

PARTIAL

NONE

CVE References

Description

Tags

Link

PHPBB Multiple HTTP Response Splitting Vulnerabilities

[Exploit](#)
[cve.report \(archive\)](#)
[text/html](#)

[🌐 BID 10753](#)

'PhpBB HTTP Response Splitting & Cross Site Scripting vulnerabilities' - MARC

[marc.info](#)
[text/html](#)

[🌐 BUGTRAQ 20040720 PhpBB HTTP Response Splitting & Cross Site Scripting vulnerabilities](#)

Secunia - Advisories - phpBB Cross Site Scripting Vulnerabilities

[web.archive.org](#)
[text/html](#)

[X SECUNIA 12114](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[🔗 XF phpbb-search-response-splitting\(16759\)](#)

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

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	2.0.2	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	2.0.6c	All	All	All
Application	Phpbb Group	Phpbb	2.0.6d	All	All	All
Application	Phpbb Group	Phpbb	2.0.7	All	All	All
Application	Phpbb Group	Phpbb	2.0.7a	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_beta1	All	All	All
Application	Phpbb Group	Phpbb	2.0_rc1	All	All	All
Application	Phpbb Group	Phpbb	2.0_rc2	All	All	All
Application	Phpbb Group	Phpbb	2.0_rc3	All	All	All
Application	Phpbb Group	Phpbb	2.0_rc4	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	2.0.2	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	2.0.6c	All	All	All
Application	Phpbb Group	Phpbb	2.0.6d	All	All	All
Application	Phpbb Group	Phpbb	2.0.7	All	All	All
Application	Phpbb Group	Phpbb	2.0.7a	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_beta1	All	All	All
Application	Phpbb Group	Phpbb	2.0_rc1	All	All	All
Application	Phpbb Group	Phpbb	2.0_rc2	All	All	All
Application	Phpbb Group	Phpbb	2.0_rc3	All	All	All
Application	Phpbb Group	Phpbb	2.0_rc4	All	All	All
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:2.0.2:*:*:*:*:*:						
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:2.0.6c:*:*:*:*:*:						
cpe:2.3:a:phpbb_group:phpbb:2.0.6d:*:*:*:*:*:						
cpe:2.3:a:phpbb_group:phpbb:2.0.7:*:*:*:*:*:						
cpe:2.3:a:phpbb_group:phpbb:2.0.7a:*:*:*:*:*:						
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_beta1:*:*:*:*:*:						
cpe:2.3:a:phpbb_group:phpbb:2.0_rc1:*:*:*:*:*:						
cpe:2.3:a:phpbb_group:phpbb:2.0_rc2:*:*:*:*:*:						
cpe:2.3:a:phpbb_group:phpbb:2.0_rc3:*:*:*:*:*:						
cpe:2.3:a:phpbb_group:phpbb:2.0_rc4:*:*:*:*:*:						
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:2.0.2:*:*:*:*:*:						

```
cpe:2.3:a:phpbb_group:phpbb:2.0_rc4:*.:.:.:.:.:
```

Next ID→