



CVE-2004-1943

Published on: 04/19/2004 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

CVE-2004-1943

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

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

PHP remote file inclusion vulnerability in album_portal.php in phpBB modified by Przemo 1.8 allows remote attackers to execute arbitrary PHP code via the phpbb_root_path parameter.

CVE-2004-1943 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

PHPBB album_portal.php Remote File Include Vulnerability

[Patch](#)
[Vendor Advisory](#)
[cve.report \(archive\)](#)
[text/html](#)

[🌐 BID 10177](#)

'phpBB modified by Przemo arbitrary code execution' - MARC

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

[🌐 BUGTRAQ 20040419 phpBB modified by Przemo arbitrary code execution](#)

IBM X-Force Exchange

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

[🔗 XF phpbb-albumportal-file-include\(15916\)](#)

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	2.0.2	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_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_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_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:2.0.3:*****:~						
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_rc4:*:*:*:*:*:*:
```

Next ID→

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