



CVE-2004-1535

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

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

CVE-2004-1535

[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 admin_cash.php for the Cash Mod module for phpBB allows remote attackers to execute arbitrary PHP code by modifying the phpbb_root_path parameter to reference a URL on a remote web server that contains the code.

CVE-2004-1535 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

IBM X-Force Exchange

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

[XF phpbb-admincashphp-file-include\(18151\)](#)

No Description Provided

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

[BUGTRAQ 20041118 Vulnerabilities in forum phpBB2 with Cash_Mod \(all ver.\)](#)

'Re: Vulnerabilities in forum phpBB2 with Cash_Mod (all ver.)' - MARC

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

[BUGTRAQ 20041118 Re: Vulnerabilities in forum phpBB2 with Cash_Mod \(all ver.\)](#)

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	2.0.2	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	2.0.9	All	All	All
Application	Phpbb Group	Phpbb	rc1	All	All	All
Application	Phpbb Group	Phpbb	rc1_pre	All	All	All
Application	Phpbb Group	Phpbb	rc2	All	All	All
Application	Phpbb Group	Phpbb	rc3	All	All	All
Application	Phpbb Group	Phpbb	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	2.0.10	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	2.0.9	All	All	All
Application	Phpbb Group	Phpbb	rc1	All	All	All
Application	Phpbb Group	Phpbb	rc1_pre	All	All	All
Application	Phpbb Group	Phpbb	rc2	All	All	All
Application	Phpbb Group	Phpbb	rc3	All	All	All
Application	Phpbb Group	Phpbb	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:2.0.10:*****:
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:2.0.9:*****:
cpe:2.3:a:phpbb_group:phpbb:rc1:*****:
cpe:2.3:a:phpbb_group:phpbb:rc1_pre:*****:
cpe:2.3:a:phpbb_group:phpbb:rc2:*****:
cpe:2.3:a:phpbb_group:phpbb:rc3:*****:
cpe:2.3:a:phpbb_group:phpbb: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:2.0.10:*****:
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:2.0.9:*****:
cpe:2.3:a:phpbb_group:phpbb:rc1:*****:

cpe:2.3:a:phpbb_group:phpbb:rc1_pre:*****:

cpe:2.3:a:phpbb_group:phpbb:rc2:*****:

cpe:2.3:a:phpbb_group:phpbb:rc3:*****:

cpe:2.3:a:phpbb_group:phpbb:rc4:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→