



# CVE-2006-4286

Published on: 08/22/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:55 PM UTC

## CVE-2006-4286

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of Mambo from Mambo contain the following vulnerability:

**\*\* DISPUTED \*\*** PHP remote file inclusion vulnerability in contentpublisher.php in the contentpublisher component (com\_contentpublisher) for Mambo allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig\_absolute\_path parameter. NOTE: this issue has been disputed by third parties who state that contentpublisher.php protects against direct request in the most recent version. The original researcher is known to be frequently inaccurate.

CVE-2006-4286 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

SecurityFocus

[www.securityfocus.com  
text/html](http://www.securityfocus.com/text/html)

[BUGTRAQ 20060817 contentpublisher Mambo Component Remote File Include Vulnerabilities](#)

SecurityFocus

[www.securityfocus.com  
text/html](http://www.securityfocus.com/text/html)

[BUGTRAQ 20060823 Re: contentpublisher Mambo Component Remote File Include Vulnerabilities](#)

**No Description Provided**

[www.osvdb.org](http://www.osvdb.org)

[OSVDB 28093](#)

**Inactive Link** **Not Archived**

SecurityReason - contentpublisher Mambo Component

[securityreason.com](http://securityreason.com)

[SREASON 1431](#)

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](mailto: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 | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.0.14         | All    | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5.0.2        | All    | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5.1.3        | All    | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5.1a         | All    | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5.1a         | a      | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5.1a         | beta   | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5.1a         | beta_2 | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5.1_1.0.9    | All    | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5.2          | All    | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5.2.1        | All    | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5.2.2        | All    | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5.2.3        | All    | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5.3h         | All    | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5.3h         | h      | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5_1.0.0      | All    | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5_1.0.1      | All    | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5_1.0.2      | All    | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5_1.0.3_beta | All    | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5_1.0.3_beta | beta   | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5_1.0.9      | All    | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.6            | rc1    | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.0.14         | All    | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5.0.2        | All    | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5.1.3        | All    | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5.1a         | All    | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5.1a         | a      | All     | All      |
| Application | <a href="#">Mambo</a> | <a href="#">Mambo</a> | 4.5.1a         | beta   | All     | All      |



|                                                                    |
|--------------------------------------------------------------------|
| cpe:2.3:a:mambo:mambo:4.5_1.0.2:~::~~::~~::~~::~~::~~:::           |
| cpe:2.3:a:mambo:mambo:4.5_1.0.3_beta:~::~~::~~::~~::~~::~~:::      |
| cpe:2.3:a:mambo:mambo:4.5_1.0.3_beta:beta:~::~~::~~::~~::~~::~~::: |
| cpe:2.3:a:mambo:mambo:4.5_1.0.9:~::~~::~~::~~::~~::~~:::           |
| cpe:2.3:a:mambo:mambo:4.6:rc1:~::~~::~~::~~::~~::~~:::             |
| cpe:2.3:a:mambo:mambo:4.0.14:~::~~::~~::~~::~~::~~:::              |
| cpe:2.3:a:mambo:mambo:4.5.0.2:~::~~::~~::~~::~~::~~:::             |
| cpe:2.3:a:mambo:mambo:4.5.1.3:~::~~::~~::~~::~~::~~:::             |
| cpe:2.3:a:mambo:mambo:4.5.1a:~::~~::~~::~~::~~::~~:::              |
| cpe:2.3:a:mambo:mambo:4.5.1a:a:~::~~::~~::~~::~~::~~:::            |
| cpe:2.3:a:mambo:mambo:4.5.1a:beta:~::~~::~~::~~::~~::~~:::         |
| cpe:2.3:a:mambo:mambo:4.5.1a:beta_2:~::~~::~~::~~::~~::~~:::       |
| cpe:2.3:a:mambo:mambo:4.5_1_1.0.9:~::~~::~~::~~::~~::~~:::         |
| cpe:2.3:a:mambo:mambo:4.5.2:~::~~::~~::~~::~~::~~:::               |
| cpe:2.3:a:mambo:mambo:4.5.2.1:~::~~::~~::~~::~~::~~:::             |
| cpe:2.3:a:mambo:mambo:4.5.2.2:~::~~::~~::~~::~~::~~:::             |
| cpe:2.3:a:mambo:mambo:4.5.2.3:~::~~::~~::~~::~~::~~:::             |
| cpe:2.3:a:mambo:mambo:4.5.3h:~::~~::~~::~~::~~::~~:::              |
| cpe:2.3:a:mambo:mambo:4.5.3h:h:~::~~::~~::~~::~~::~~:::            |
| cpe:2.3:a:mambo:mambo:4.5_1.0.0:~::~~::~~::~~::~~::~~:::           |
| cpe:2.3:a:mambo:mambo:4.5_1.0.1:~::~~::~~::~~::~~::~~:::           |
| cpe:2.3:a:mambo:mambo:4.5_1.0.2:~::~~::~~::~~::~~::~~:::           |
| cpe:2.3:a:mambo:mambo:4.5_1.0.3_beta:~::~~::~~::~~::~~::~~:::      |
| cpe:2.3:a:mambo:mambo:4.5_1.0.3_beta:beta:~::~~::~~::~~::~~::~~::: |
| cpe:2.3:a:mambo:mambo:4.5_1.0.9:~::~~::~~::~~::~~::~~:::           |
| cpe:2.3:a:mambo:mambo:4.6:rc1:~::~~::~~::~~::~~::~~:::             |

No vendor comments have been submitted for this CVE

© 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](#)