

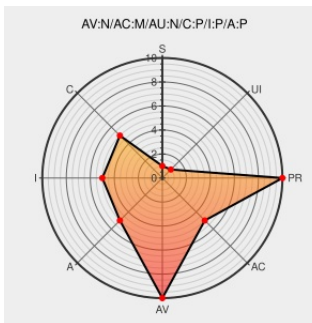


CVE-2010-1715

Published on: 05/04/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:05 PM UTC

CVE-2010-1715

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

Certain versions of [Joomla!](#) from [Joomla](#) contain the following vulnerability:

Directory traversal vulnerability in the Online Examination (aka Online Exam or com_onlineexam) component 1.5.0 for Joomla! allows remote attackers to read arbitrary files via a .. (dot dot) in the controller parameter to index.php. NOTE: some of these details are obtained from third party information.

CVE-2010-1715 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Files ~ Packet Storm

[Exploit](#)
[packetstormsecurity.org](#)
[text/plain](#)

[MISC](#)
[packetstormsecurity.org/1004-exploits/joomlaonlineexam-lfi.txt](#)

IBM X-Force Exchange

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

[XF comonlineexam-controller-file-include\(57677\)](#)

Joomla Component Online Exam com_onlineexam Local File Inclusion Vulnerability

[Exploit](#)
[www.exploit-db.com](#)
[Proof of Concept](#)
[text/html](#)

[EXPLOIT-DB 12174](#)

No Description Provided

[www.osvdb.org](#)

[OSVDB 63659](#)

[Inactive Link](#) [Not Archived](#)

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Joomla	Joomla!	All	All	All	All
Application	Joomla	Joomla!	All	All	All	All
Application	Joomla	Joomla!	All	All	All	All
Application	Pucit.edu	Com Onlineexam	1.5.0	All	All	All
Application	Pucit.edu	Com Onlineexam	1.5.0	All	All	All
cpe:2.3:a:joomla:joomla!:*****:.*:						
cpe:2.3:a:joomla:joomla\!:*.*.*.*.*.*:.*:						
cpe:2.3:a:joomla:joomla\!:*.*.*.*.*.*:.*:						
cpe:2.3:a:pucit.edu:com_onlineexam:1.5.0:*****:.*:						
cpe:2.3:a:pucit.edu:com_onlineexam:1.5.0:*****:.*:						