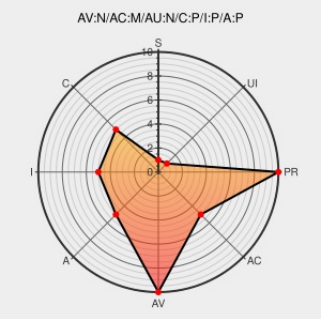
CVE-2006-2286

Published on: 05/09/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:08 PM UTC

CVE-2006-2286

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Dokeos from Dokeos contain the following vulnerability:

Multiple PHP remote file inclusion vulnerabilities in claro_init_global.inc.php in Dokeos 1.6.3 and earlier, and Dokeos community release 2.0.3, allow remote attackers to execute arbitrary PHP code via a URL in the (1) rootSys and (2) clarolineRepositorySys parameters, and possibly the (3) lang_path, (4) extAuthSource, (5) thisAuthSource, (6) main_configuration_file_path, (7) phpDigIncCn, and (8) drs parameters to (a) testheaderpage.php and (b) resourcelinker.inc.php.

CVE-2006-2286 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Dokeos File Inclusion Vulnerabilities - Advisories - Secunia	Vendor Advisory, web.archive.org, text/html	SECUNIA 19576
Page Not Found - Dokeos	web.archive.org, text/html, Inactive Link, Not Archived	CONFIRM www.dokeos.com/forum/viewtopic.php?t=6848
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF dokeos-multiple-file-include(25740)
Webmail : Solution de messagerie professionnelle -	Vendor Advisory	VUPEN ADV-2006-1303

OVHcloud- OVH	www.vupen.com text/html	
Security - Dokeos	www.dokeos.com text/html	CONFIRM www.dokeos.com/wiki/index.php/Security

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	Dokeos	Dokeos	All	All	All	All
Application	Dokeos	Dokeos Community Release	2.0.3	All	All	All
Application	Dokeos	Dokeos Community Release	2.0.3	All	All	All

cpe:2.3:a:dokeos:dokeos:*:*:*:*:*:*:*:*:

cpe:2.3:a:dokeos:dokeos_community_release:2.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:dokeos:dokeos_community_release:2.0.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→