



CVE-2006-2284

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

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

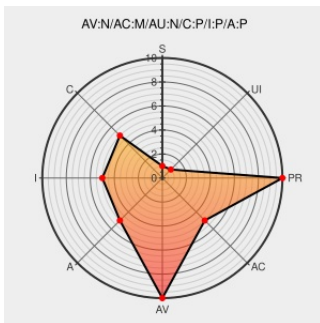
CVE-2006-2284

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Multiple PHP remote file inclusion vulnerabilities in Claroline 1.7.5 allow remote attackers to execute arbitrary PHP code via a URL in the (1) `clarolineRepositorySys` parameter in `ldap.inc.php` and the (2) `claro_CasLibPath` parameter in `casProcess.inc.php`.

CVE-2006-2284 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

No Description Provided

Tags

www.osvdb.org

Link

[OSVDB 25316](#)

Inactive Link **Not Archived**

SecurityReason

securityreason.com

[text/html](#)

SREASON 875

IBM X-Force Exchange

exchange.xforce.ibmcloud.com

[text/html](#)

XF claroline-ldapinc-casprocessinc-file-include(26280)

Webmail : Solution de messagerie professionnelle
- OVHcloud- OVH

www.vupen.com

[text/html](#)

[VUPEN ADV-2006-1701](#)

SecurityFocus

www.securityfocus.com

[text/html](#)

[BUGTRAQ 20060508 Claroline Open Source e-Learning 1.7.5 Remote File Include](#)

Claroline e-Learning 1.7.5 (ldap.inc.php) Remote

www.exploit-db.com

EXPLOIT-DB 1766

File Inclusion Exploit	Proof of Concept text/html	
Claroline File Inclusion Vulnerabilities - Advisories - Secunia	Patch Vendor Advisory web.archive.org text/html	 SECUNIA 20003
Claroline Multiple Remote File Include Vulnerabilities	Exploit Patch cve.report (archive) text/html	 BID 17873

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	Claroline	Claroline	1.5	All	All	All
Application	Claroline	Claroline	1.5.3	All	All	All
Application	Claroline	Claroline	1.5.4	All	All	All
Application	Claroline	Claroline	1.6	All	All	All
Application	Claroline	Claroline	1.6_beta	All	All	All
Application	Claroline	Claroline	1.6_rc1	All	All	All
Application	Claroline	Claroline	1.7.2	All	All	All
Application	Claroline	Claroline	1.7.4	All	All	All
Application	Claroline	Claroline	1.7.5	All	All	All
Application	Claroline	Claroline	1.5	All	All	All
Application	Claroline	Claroline	1.5.3	All	All	All
Application	Claroline	Claroline	1.5.4	All	All	All
Application	Claroline	Claroline	1.6	All	All	All
Application	Claroline	Claroline	1.6_beta	All	All	All
Application	Claroline	Claroline	1.6_rc1	All	All	All
Application	Claroline	Claroline	1.7.2	All	All	All
Application	Claroline	Claroline	1.7.4	All	All	All
Application	Claroline	Claroline	1.7.5	All	All	All
Application	Dokeos	Dokeos	1.4	All	All	All
Application	Dokeos	Dokeos	1.5	All	All	All
Application	Dokeos	Dokeos	1.5.3	All	All	All

Application	Dokeos	Dokeos	1.5.4	All	All	All
Application	Dokeos	Dokeos	1.5.5	All	All	All
Application	Dokeos	Dokeos	1.6.4	All	All	All
Application	Dokeos	Dokeos	1.6_rc2	All	All	All
Application	Dokeos	Dokeos	1.4	All	All	All
Application	Dokeos	Dokeos	1.5	All	All	All
Application	Dokeos	Dokeos	1.5.3	All	All	All
Application	Dokeos	Dokeos	1.5.4	All	All	All
Application	Dokeos	Dokeos	1.5.5	All	All	All
Application	Dokeos	Dokeos	1.6.4	All	All	All
Application	Dokeos	Dokeos	1.6_rc2	All	All	All
cpe:2.3:a:claroline:claroline:1.5:*****:						
cpe:2.3:a:claroline:claroline:1.5.3:*****:						
cpe:2.3:a:claroline:claroline:1.5.4:*****:						
cpe:2.3:a:claroline:claroline:1.6:*****:						
cpe:2.3:a:claroline:claroline:1.6_beta:*****:						
cpe:2.3:a:claroline:claroline:1.6_rc1:*****:						
cpe:2.3:a:claroline:claroline:1.7.2:*****:						
cpe:2.3:a:claroline:claroline:1.7.4:*****:						
cpe:2.3:a:claroline:claroline:1.7.5:*****:						
cpe:2.3:a:claroline:claroline:1.5:*****:						
cpe:2.3:a:claroline:claroline:1.5.3:*****:						
cpe:2.3:a:claroline:claroline:1.5.4:*****:						
cpe:2.3:a:claroline:claroline:1.6:*****:						
cpe:2.3:a:claroline:claroline:1.6_beta:*****:						
cpe:2.3:a:claroline:claroline:1.6_rc1:*****:						
cpe:2.3:a:claroline:claroline:1.7.2:*****:						
cpe:2.3:a:claroline:claroline:1.7.4:*****:						
cpe:2.3:a:claroline:claroline:1.7.5:*****:						
cpe:2.3:a:dokeos:dokeos:1.4:*****:						
cpe:2.3:a:dokeos:dokeos:1.5:*****:						

cpe:2.3:a:dokeos:dokeos:1.5:*:*:*:*:*:
cpe:2.3:a:dokeos:dokeos:1.5.3:*:*:*:*:*:
cpe:2.3:a:dokeos:dokeos:1.5.4:*:*:*:*:*:
cpe:2.3:a:dokeos:dokeos:1.5.5:*:*:*:*:*:
cpe:2.3:a:dokeos:dokeos:1.6.4:*:*:*:*:*:
cpe:2.3:a:dokeos:dokeos:1.6_rc2:*:*:*:*:*:
cpe:2.3:a:dokeos:dokeos:1.4:*:*:*:*:*:
cpe:2.3:a:dokeos:dokeos:1.5:*:*:*:*:*:
cpe:2.3:a:dokeos:dokeos:1.5.3:*:*:*:*:*:
cpe:2.3:a:dokeos:dokeos:1.5.4:*:*:*:*:*:
cpe:2.3:a:dokeos:dokeos:1.5.5:*:*:*:*:*:
cpe:2.3:a:dokeos:dokeos:1.6.4:*:*:*:*:*:
cpe:2.3:a:dokeos:dokeos:1.6_rc2:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)