



CVE-2005-1375

Published on: 05/02/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-1375

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

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

Multiple SQL injection vulnerabilities in Claroline 1.5.3 through 1.6 Release Candidate 1, and possibly Dokeos, allow remote attackers to execute arbitrary SQL commands via (1) learningPath.php, (2) learningPathAdmin.php, (3) learnPath_details.php, (4) modules_pool.php, (5) module.php, (6) ulInfo parameter in userInfo.php, or (7) exo_id parameter to exercises_details.php.

CVE-2005-1375 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Secunia - Advisories - Claroline Multiple Vulnerabilities	Exploit Patch web.archive.org text/html	X SECUNIA 15161
'ZRCSA-200501 - Multiple vulnerabilities in Claroline' - MARC	marc.info text/html	BUGTRAQ 20050427 ZRCSA-200501 - Multiple vulnerabilities in Claroline
SecurityTracker.com Archives - Claroline Lets Remote Users Execute Arbitrary Commands, View Files, Inject SQL Commands, and Conduct Cross-Site Scripting Attacks	Exploit Patch securitytracker.com text/html	SECTrack 1013822

Secunia - Advisories - Dokeos Multiple Vulnerabilities	web.archive.org text/html	 SECUNIA 15725
Claroline E-Learning Application Multiple Remote Input Validation Vulnerabilities	Exploit Patch cve.report (archive) text/html	 BID 13407
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF claroline-multiple-sql-injection(20298)
Page non trouvée - Claroline	Patch web.archive.org text/html Inactive Link Not Archived	 CONFIRM www.claroline.net/news.php#85

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	1.5.3	All	All	All
Application	Claroline	Claroline	1.6_beta	All	All	All
Application	Claroline	Claroline	1.6_rc1	All	All	All
Application	Claroline	Claroline	1.5.3	All	All	All
Application	Claroline	Claroline	1.6_beta	All	All	All
Application	Claroline	Claroline	1.6_rc1	All	All	All
cpe:2.3:a:claroline:claroline:1.5.3:****:*:*:						
cpe:2.3:a:claroline:claroline:1.6_beta:****:*:*:						
cpe:2.3:a:claroline:claroline:1.6_rc1:****:*:*:						
cpe:2.3:a:claroline:claroline:1.5.3:****:*:*:						
cpe:2.3:a:claroline:claroline:1.6_beta:****:*:*:						
cpe:2.3:a:claroline:claroline:1.6_rc1:****:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)