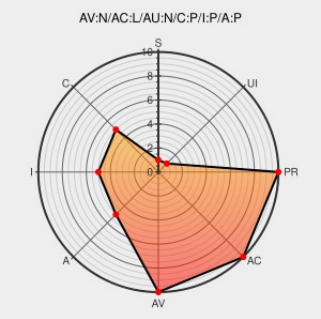
CVE-2006-1594

Published on: 04/03/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:59 PM UTC

CVE-2006-1594

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



Certain versions of Claroline from Claroline contain the following vulnerability:

Multiple directory traversal vulnerabilities in document/rqmkhtml.php in Claroline 1.7.4 and earlier allow remote attackers to use ".." (dot dot) sequences to (1) read arbitrary files via the file parameter in a rqEditHtml command to document/rqmkhtml.php or (2) execute arbitrary code via the includePath parameter to learnPath/include/scormExport.inc.php.

CVE-2006-1594 has been assigned by 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
Claroline <= 1.7.4 (scormExport.inc.php) Remote Code Execution Exploit	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 1627
Claroline Rqmkhtml.PHP Information Disclosure Vulnerability	cve.report (archive) text/html	BID 17343
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF claroline-rqmkhtml-directory-traversal(25561)
Error 404 :(	Exploit retrogod.altervista.org text/plain Inactive Link Not Archived	MISC retrogod.altervista.org/claroline_174_incl_xpl.html

Claroline Multiple Vulnerabilities - Advisories - Secunia	Exploit Vendor Advisory web.archive.org text/html	SECUNIA 19461
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-1187

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	1.5	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	All	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:1.5:*:*:*:*:*:*:*:

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:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→