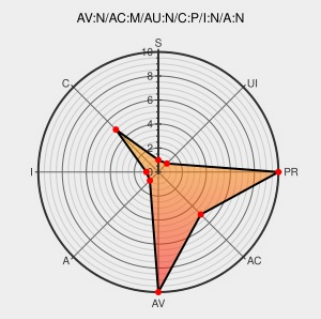
CVE-2006-1595

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

Last Modified on: 03/23/2021 11:25:00 PM UTC

CVE-2006-1595

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



Certain versions of Claroline from Claroline contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in document/rqmkhtml.php in Claroline 1.7.4 and earlier allows remote attackers to read arbitrary files via ".." sequences in the file parameter in a rqEditHtml command.

CVE-2006-1595 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

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

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
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF claroline-rqmkhtml-xss(25562)
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 24284
No Description Provided	Exploit web.archive.org text/html Inactive Link Not Archived	FULLDISC 20060331 Re: [Full-disclosure] Claroline <= 1.7.4 (scormExport.inc.php) Remote Code Execution Exploit by rgod
Claroline RQMKHTML.PHP Cross-Site	Exploit	BID 17344

Scripting Vulnerability	cve.report (archive) text/html	
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
No Description Provided	Exploit www.osvdb.org Inactive Link Not Archived	OSVDB 24285
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-1187

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→