



CVE-2006-4844

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2006-4844
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-09-19 01:07:00 UTC
Updated	2017-07-20 01:33:00 UTC
Description	PHP remote file inclusion vulnerability in inc/claro_init_local.inc.php in Claroline 1.7.7 and earlier, as used in Dokeos and pc

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Claroline	Claroline	1.2	All	All	All
Application	Claroline	Claroline	1.3	All	All	All
Application	Claroline	Claroline	1.4	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	All	All	All
Application	Claroline	Claroline	1.7.1	All	All	All
Application	Claroline	Claroline	1.7.2	All	All	All
Application	Claroline	Claroline	1.7.3	All	All	All
Application	Claroline	Claroline	1.7.4	All	All	All
Application	Claroline	Claroline	1.7.5	All	All	All
Application	Claroline	Claroline	1.7.6	All	All	All
Application	Claroline	Claroline	1.2	All	All	All

Application	Claroline	Claroline	1.3	All	All	All
Application	Claroline	Claroline	1.4	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	All	All	All
Application	Claroline	Claroline	1.7.1	All	All	All
Application	Claroline	Claroline	1.7.2	All	All	All
Application	Claroline	Claroline	1.7.3	All	All	All
Application	Claroline	Claroline	1.7.4	All	All	All
Application	Claroline	Claroline	1.7.5	All	All	All
Application	Claroline	Claroline	1.7.6	All	All	All
Application	Claroline	Claroline	All	All	All	All
Application	Dokeos	Open Source Learning And Knowledge Management Tool	1.4	All	All	All
Application	Dokeos	Open Source Learning And Knowledge Management Tool	1.5	All	All	All
Application	Dokeos	Open Source Learning And Knowledge Management Tool	1.5.3	All	All	All
Application	Dokeos	Open Source Learning And Knowledge Management Tool	1.5.4	All	All	All
Application	Dokeos	Open Source Learning And Knowledge Management Tool	1.5.5	All	All	All
Application	Dokeos	Open Source Learning And Knowledge Management Tool	1.6.4	All	All	All
Application	Dokeos	Open Source Learning And Knowledge Management Tool	1.6.4_p1	All	All	All
Application	Dokeos	Open Source Learning And Knowledge Management Tool	1.6.5	All	All	All
Application	Dokeos	Open Source Learning And Knowledge Management Tool	1.6_rc2	All	All	All
Application	Dokeos	Open Source Learning And Knowledge Management Tool	1.4	All	All	All
Application	Dokeos	Open Source Learning And Knowledge Management Tool	1.5	All	All	All
Application	Dokeos	Open Source Learning And Knowledge Management Tool	1.5.3	All	All	All
Application	Dokeos	Open Source Learning And Knowledge Management Tool	1.5.4	All	All	All
Application	Dokeos	Open Source Learning And Knowledge Management Tool	1.5.5	All	All	All
Application	Dokeos	Open Source Learning And Knowledge Management Tool	1.6.4	All	All	All
Application	Dokeos	Open Source Learning And Knowledge Management Tool	1.6.4_p1	All	All	All
Application	Dokeos	Open Source Learning And Knowledge Management Tool	1.6.5	All	All	All
Application	Dokeos	Open Source Learning And Knowledge Management Tool	1.6_rc2	All	All	All

References

Reference	Source	Link	Tags
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	Vendor
Page non trouvée - Claroline	CONFIRM	www.claroline.net	Patched
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
Contact Support	MISC	www.gulftech.org	Exploit
Dokeos "extAuthSource[newUser]" File Inclusion Vulnerability - Advisories - Secunia	SECUNIA	secunia.com	Vendor
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	Vendor
Contact Support	MISC	www.gulftech.org	
Claroline Claro_Init_Local.Inc.PHP Remote File Include Vulnerability	BID	www.securityfocus.com	Patched
Claroline "extAuthSource[newUser]" File Inclusion Vulnerability - Advisories - Secunia	SECUNIA	secunia.com	Exploit
CVE Program record	CVE.ORG	www.cve.org	Canonical
NVD vulnerability detail	NVD	nvd.nist.gov	Canonical

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org/). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/mitre).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report