



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

**S . G . D . S . N**  
*Agence nationale de la sécurité  
des systèmes d'information*  
**CERTA**

Paris, le 03 avril 2006  
N° CERTA-2006-AVI-133

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Claroline

---

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>  
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-133>

---

### Gestion du document

Référence	CERTA-2006-AVI-133
Titre	Vulnérabilités dans Claroline
Date de la première version	03 avril 2006
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

## 1 Risque

- Exécution de code arbitraire à distance ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

Claroline versions 1.7.x, 1.6.x et 1.5.x.

## 3 Résumé

Trois vulnérabilités découvertes dans Claroline permettent l'exécution de code arbitraire à distance ou de porter atteinte à la confidentialité des données.

## 4 Description

Claroline est une application basée sur Php et MySQL qui permet la création de cours en ligne.

Trois vulnérabilités affectant les fichiers `rqmkhtml.php` et `scormExport.inc.php` permettent l'exécution de code arbitraire à distance ou de porter atteinte à la confidentialité des données.

## **5 Solution**

Appliquer le correctif de l'éditeur (voir section Documentation).

## **6 Documentation**

- Correctif pour les versions 1.7 :  
<http://www.claroline.net/dlarea/claroline.patch17401.zip>
- Correctif pour les versions 1.6 :  
<http://www.claroline.net/dlarea/claroline.patch16301.zip>
- Correctif pour les versions 1.5 :  
<http://www.claroline.net/dlarea/claroline.patch15401.zip>

## **Gestion détaillée du document**

**03 avril 2006** version initiale.