

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-192>

Gestion du document

Référence	CERTA-2006-AVI-192
Titre	Vulnérabilités dans Claroline
Date de la première version	10 mai 2006
Date de la dernière version	–
Source(s)	Discussion sur le forum du site de Claroline
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.

2 Systèmes affectés

Claroline versions 1.7.x et 1.6.x.

3 Description

Des vulnérabilités de type `php include` ont été découvertes dans les versions 1.6.x et 1.7.x de *Claroline*. L'exploitation de ces vulnérabilités permet l'exécution de code arbitraire à distance sur le serveur *Claroline*.

4 Solution

Appliquer les correctifs disponibles sur le site de l'éditeur (cf. section Documentation).

5 Documentation

- Site de Claroline :
<http://www.claroline.net/>
- Correctif pour les versions 1.7 :
<http://www.claroline.net/dlarea/claroline.patch17501.zip>
- Correctif pour les versions 1.6 :
<http://www.claroline.net/dlarea/claroline.patch16401.zip>

Gestion détaillée du document

10 mai 2006 version initiale.