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 septembre 2007
N° CERTA-2007-AVI-386

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Claroline

Gestion du document

Référence	CERTA-2007-AVI-386
Titre	Vulnérabilités dans Claroline
Date de la première version	03 septembre 2007
Date de la dernière version	–
Source(s)	Notes de changement de version 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 ;
- attaques de type *cross-site scripting*.

2 Systèmes affectés

Claroline versions 1.8.5 et antérieures.

3 Résumé

Plusieurs vulnérabilités dans *Claroline* permettent de réaliser des attaques de type *cross-site scripting* et d'exécuter des fichiers locaux.

4 Description

Plusieurs vulnérabilités ont été découvertes dans *Claroline* versions 1.8.5 et antérieures. Certaines d'entre elles, présentes dans les fichiers `adminusers.php`, `advancedUserSearch.php` et `campusProblem.php` du répertoire `admin` permettent de réaliser des attaques de type *cross-site scripting* (injection de code indirecte).

Une autre vulnérabilité, présente dans le fichier `language.lib.php` permet d'inclure des fichiers locaux. Ceci peut provoquer l'affichage de leur contenu et, dans certains cas, une exécution de code arbitraire à distance sera possible.

5 Solution

Mettre à jour en version 1.8.6 (cf. section Documentation).

6 Documentation

- Site du projet *Claroline* :
  http://www.claroline.net/
- Notes de changement de version de *Claroline* :
  http://www.claroline.net/wiki/index.php/Changelog_1.8.x#Security

Gestion détaillée du document

03 septembre 2007 version initiale.