Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 mai 2011
N° CERTA-2011-AVI-305

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Moodle

Gestion du document

Référence	CERTA-2011-AVI-305
Titre	Multiples vulnérabilités dans Moodle
Date de la première version	20 mai 2011
Date de la dernière version	–
Source(s)	Annonce des nouvelles versions de Moodle du 19 mai 2011
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

- Déni de service à distance ;
- atteinte à la confidentialité des données ;
- injection de code indirecte à distance.

2 Systèmes affectés

- *Moodle* versions 2.0.x antérieures à 2.0.3 ;
- *Moodle* versions 1.9.x antérieures à 1.9.12.

3 Résumé

De multiples vulnérabilités dans *Moodle* permettent, entre autres, de réaliser un déni de service ou une injection de code indirecte à distance.

4 Description

De multiples vulnérabilités ont été découvertes dans *Moodle* :

- un enseignant peut voir les rapports de quizz de tous les étudiants, même ceux qui ne sont pas dans ses groupes (MSA-11-0013) ;
- les adresses de messagerie des utilisateurs sont affichées dans la page de profil, lorsqu'elles ne devraient apparaître qu'aux membres du cours seulement (MSA-11-0014) ;
- plusieurs injections de code indirectes sont possibles (MSA-11-0015) ;
- un utilisateur légitime peut créer plusieurs enregistrements invalides dans la base de données, ce qui peut conduire à un déni de service (MSA-11-0016) ;
- un utilisateur légitime peut remplir la table des commentaires dans la base de données avec des enregistrements invalides (MSA-11-0017).

5 Solution

Les versions 2.0.3 et 1.9.12 de *Moodle* corrigent ces vulnérabilités.

6 Documentation

- Annonce des nouvelles versions de Moodle du 19 mai 2011 :
  http://moodle.org/mod/forum/discuss.php?d=175658
- Bulletins de sécurité Moodle MSA-11-0013 à MSA-11-0017 :
  http://moodle.org/mod/forum/discuss.php?d=175590
  http://moodle.org/mod/forum/discuss.php?d=175591
  http://moodle.org/mod/forum/discuss.php?d=175592
  http://moodle.org/mod/forum/discuss.php?d=175593
  http://moodle.org/mod/forum/discuss.php?d=175594

Gestion détaillée du document

20 mai 2011 version initiale.