Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 décembre 2011
N° CERTA-2011-AVI-717

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Moodle

Gestion du document

Référence	CERTA-2011-AVI-717
Titre	Vulnérabilités dans Moodle
Date de la première version	23 décembre 2011
Date de la dernière version	–
Source	Bulletins de sécurité Moodle MSA-11-0042 à MSA-11-0054 du 06 décembre 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

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Moodle 1.x et 2.x.

3 Résumé

Plusieurs vulnérabilités dans Moodle permettent le contournement de la politique de sécurité et la divulgation de données.

4 Description

Plusieurs vulnérabilités affectent Moodle :

- le nom du compte d'un utilisateur est affiché par le wiki au lieu du nom à afficher ;
- le calendrier permet la redirection vers une adresse hors du site Moodle ;

- des jetons d'authentification peuvent être lus sans droit ;
- plusieurs fonctionnalités ne restreignent pas correctement les accès ;
- le changement de mot de passe peut se faire en utilisant une communication non protégée ;
- des injections sont possibles dans les en-têtes HTTP ;
- la politique de mot de passe peut conduire à des mots de passe vides (longueur nulle) ;
- le masquage des mèls peut être contourné ;
- des vulnérabilités affectent la sauvegarde et l'impression ;
- les commandes en ligne peuvent être inutilisables dans certaines conditions.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletins de sécurité Moodle MSA-11-0042 à MSA-11-0054 du 06 décembre 2011 :
  http://moodle.org/mod/forum/discuss.php?d=191747
  http://moodle.org/mod/forum/discuss.php?d=191748
  http://moodle.org/mod/forum/discuss.php?d=191750
  http://moodle.org/mod/forum/discuss.php?d=191751
  http://moodle.org/mod/forum/discuss.php?d=191752
  http://moodle.org/mod/forum/discuss.php?d=191754
  http://moodle.org/mod/forum/discuss.php?d=191755
  http://moodle.org/mod/forum/discuss.php?d=191756
  http://moodle.org/mod/forum/discuss.php?d=191758
  http://moodle.org/mod/forum/discuss.php?d=191759
  http://moodle.org/mod/forum/discuss.php?d=191760
  http://moodle.org/mod/forum/discuss.php?d=191761
  http://moodle.org/mod/forum/discuss.php?d=191762

Gestion détaillée du document

23 décembre 2011 version initiale.