

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Moodle

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-2010-AVI-278>

Gestion du document

Référence	CERTA-2010-AVI-278-001
Titre	Vulnérabilités dans Moodle
Date de la première version	22 juin 2010
Date de la dernière version	29 juin 2010
Source(s)	Bulletin de sécurité Moodle MSA-10-0010 à 0013 du 17 juin 2010
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

- Atteinte à l'intégrité des données ;
- injection de requêtes illégitimes par rebond ;
- injection de code indirecte à distance.

2 Systèmes affectés

Moodle, versions antérieures à la version 1.8.13 (branche 1.8) et à la version 1.9.9 (branche 1.9).

3 Résumé

Plusieurs vulnérabilités présentes dans Moodle permettent de réaliser de l'injection de code indirecte, de l'injection de requêtes illégitimes par rebond et des atteintes à l'intégrité des données.

4 Description

Plusieurs vulnérabilités sont présentes dans Moodle :

- quand les identifiants des utilisateurs peuvent comporter des caractères non ASCII, une interface de contrôle d'accès permet l'injection de code indirecte ;

- un défaut de filtrage des entrées dans le module de blog permet l'injection de code indirecte ;
- un défaut de filtrage des URI VBscript permet à un utilisateur malveillant ayant un compte de réaliser l'injection de code indirecte ;
- un défaut de vérification dans un module de quizz permet d'injecter des requêtes illégitimes par rebond et de détruire des données.

5 Solution

Migrer en version 1.8.13 ou 1.9.9.

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

6 Documentation

- Bulletin de sécurité Moodle MSA-10-0010 du 17 juin 2010 :
<http://www.moodle.org/mod/forum/discuss.php?d=152366>
- Bulletin de sécurité Moodle MSA-10-0011 du 17 juin 2010 :
<http://www.moodle.org/mod/forum/discuss.php?d=152367>
- Bulletin de sécurité Moodle MSA-10-0012 du 17 juin 2010 :
<http://www.moodle.org/mod/forum/discuss.php?d=152368>
- Bulletin de sécurité Moodle MSA-10-0013 du 17 juin 2010 :
<http://www.moodle.org/mod/forum/discuss.php?d=152369>
- Référence CVE CVE-2010-2228 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2228>
- Référence CVE CVE-2010-2229 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2229>
- Référence CVE CVE-2010-2230 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2230>
- Référence CVE CVE-2010-2231 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2231>

Gestion détaillée du document

22 juin 2010 version initiale.

29 juin 2010 ajout des références CVE.