



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 avril 2007
N° CERTA-2007-AVI-171

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités sur Dotclear

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-2007-AVI-171>

Gestion du document

Référence	CERTA-2007-AVI-171
Titre	Vulnérabilités sur Dotclear
Date de la première version	13 avril 2007
Date de la dernière version	–
Source(s)	Mise à jour 1.2.6 de Dotclear
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 indirecte de code.

2 Systèmes affectés

DotClear versions antérieures à 1.2.6.

3 Résumé

Deux vulnérabilités permettant une exécution indirecte de code (XSS) ont été découvertes dans DotClear.

4 Description

Deux vulnérabilités dans DotClear permettent à une personne malintentionnée d'effectuer une attaque de type exécution indirecte de code (XSS). Ces failles sont dues à une mauvaise vérification de certains paramètres dans les pages `dotclear/ecrire/trackback.php` et `tools/thememng/index.php`.

5 Solution

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

6 Documentation

- Mise à jour de sécurité DotClear 1.2.6 :
<http://www.dotclear.net/log/post/2007/04/10/Dotclear-126>

Gestion détaillée du document

13 avril 2007 version initiale.