

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-2006-AVI-233>

Gestion du document

Référence	CERTA-2006-AVI-233
Titre	Vulnérabilité de DotClear
Date de la première version	09 juin 2006
Date de la dernière version	–
Source(s)	Bulletin de mise à jour du projet DotClear du 6 juin 2006
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.

2 Systèmes affectés

Les versions de DotClear antérieures à 1.2.5.

3 Description

Une vulnérabilité a été identifiée dans l'outil de gestion de bloc-notes (aussi appelés blogs) DotClear. Il ne vérifie pas correctement les valeurs entrées pour le paramètre `blog_dc_path` dans le script `layout/prepend.php`. Un utilisateur malveillant peut tirer partie de cette propriété pour inclure des fichiers et exécuter du code PHP arbitraire. Ceci nécessite d'avoir activé au préalable PHP5 avec les valeurs `register_globals` et `allow_url_fopen` à 1.

4 Solution

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

5 Documentation

- Référence CVE CVE-2006-2866 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2866>
- Bulletin de mise à jour du projet DotClear du 6 juin 2006 :
<http://www.dotclear.net/download.html>

Gestion détaillée du document

09 juin 2006 version initiale.