



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 02 décembre 2005  
N° CERTA-2005-AVI-479

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans 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-2005-AVI-479>

---

### Gestion du document

Référence	CERTA-2005-AVI-479
Titre	Vulnérabilité dans DotClear
Date de la première version	02 décembre 2005
Date de la dernière version	–
Source(s)	Mise à jour de sécurité DotClear du 30 novembre 2005
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 ;
- injection de code SQL.

## 2 Systèmes affectés

DotClear 1.x.

## 3 Résumé

Une vulnérabilité dans DotClear permet à un utilisateur mal intentionné d'injecter du code SQL arbitraire à distance.

## 4 Description

DotClear est un outil de publication sur l'Internet de type Weblog.

Une vulnérabilité dans la validation des paramètres fournit par le cookie du poste client permet à l'utilisateur d'exécuter à distance, sur le serveur vulnérable, du code SQL arbitraire à distance.

## **5 Solution**

Appliquer la mise à jour de sécurité DotClear en passant à la version 1.2.3 disponible à l'adresse suivante :  
<http://www.dotclear.net/download.html>

## **6 Documentation**

- Mise à jour de sécurité DotClear v1.2.3 du 30 novembre 2005 :  
<http://www.dotclear.net/download.html>

## **Gestion détaillée du document**

**02 décembre 2005** version initiale.