

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Dokeos

---

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-2008-AVI-117>

---

### Gestion du document

Référence	CERTA-2008-AVI-117
Titre	Vulnérabilités dans Dokeos
Date de la première version	07 mars 2008
Date de la dernière version	–
Source(s)	Page sécurité du site de Dokeos
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 indirecte.

## 2 Systèmes affectés

*Dokeos* versions 1.8.4 SP2 et antérieures.

## 3 Résumé

Plusieurs vulnérabilités dans *Dokeos* permettent l'exécution de code arbitraire à distance et l'injection de code indirecte (*cross site scripting*).

## 4 Description

Plusieurs vulnérabilités ont été découvertes dans *Dokeos*. L'exploitation de ces vulnérabilités permet l'exécution de code arbitraire à distance ou la réalisation d'attaques de type *cross site scripting*.

## **5 Solution**

Se référer à la page sécurité du site de *Dokeos* pour l'obtention du correctif SP3 (cf. section Documentation).

## **6 Documentation**

- Page sécurité du site de *Dokeos* :  
<http://www.dokeos.com/wiki/index.php/Security>
- Correctif SP3 :  
<http://www.dokeos.com/download/dokeos-1.8.4-SP3.zip>

## **Gestion détaillée du document**

**07 mars 2008** version initiale.