

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans TikiWiki

---

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-2011-AVI-657>

---

### Gestion du document

|                             |   |
|-----------------------------|---|
| Référence                   | CERTA-2011-AVI-657  |
| Titre                       | Vulnérabilités dans TikiWiki  |
| Date de la première version | 22 novembre 2011  |
| Date de la dernière version | –   |
| Source                      | Liste des changements de la version de TikiWiki du 11 novembre 2011 |
| 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

Injection de code indirecte à distance.

## 2 Systèmes affectés

TikiWiki, versions antérieures à la version 8.1.

## 3 Résumé

TikiWiki est vulnérable à de l'injection de code indirecte à distance.

## 4 Description

Des scripts PHP de TikiWiki utilisent des entrées contenues dans l'URL. Deux d'entre eux ne filtrent pas correctement ces entrées. Ces insuffisances sont exploitables par un utilisateur malveillant pour réaliser de l'injection de code indirecte à distance (XSS).

## **5 Solution**

La version 8.1 de TikiWiki corrige ces vulnérabilités.

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

## **6 Documentation**

- Liste des changements de la version de TikiWiki du 11 novembre 2011 :  
<http://tiki.org/ReleaseNotes8.1>

## **Gestion détaillée du document**

**22 novembre 2011** version initiale.