



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 30 juillet 2010  
N° CERTA-2010-AVI-346

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans MediaWiki

---

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-2010-AVI-346>

---

### Gestion du document

Référence	CERTA-2010-AVI-346
Titre	Vulnérabilités dans MediaWiki
Date de la première version	30 juillet 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité MediaWiki du 28 juillet 2010
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

- Atteinte à la confidentialité des données ;
- injection de code indirecte à distance.

## 2 Systèmes affectés

- MediaWiki versions antérieures à la 1.15.5 ;
- MediaWiki versions antérieures à la 1.16.0.

## 3 Résumé

Deux vulnérabilités dans MediaWiki permettent à une personne malintentionnée de porter atteinte à la confidentialité des données ou d'effectuer une injection de code indirecte.

## 4 Description

Deux vulnérabilités ont été découvertes dans MediaWiki :

- une erreur dans la gestion du paramètre *Cache-Control* du fichier *api.php* permet de porter atteinte à la confidentialité des données ;
- une vulnérabilité, de type injection de code indirecte, a été corrigée dans le fichier *profileinfo.php*. Celle-ci n'est exploitable que si le paramètre *\$wgEnableProfileInfo = True* est placé dans le fichier *LocalSettings.php*.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité MediaWiki du 28 juillet 2010 :  
<http://lists.wikimedia.org/pipermail/mediawiki-announce/2010-july/000092.html>

## Gestion détaillée du document

**30 juillet 2010** version initiale.