Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 février 2006
N° CERTA-2006-AVI-058

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans SPIP

Gestion du document

Référence	CERTA-2006-AVI-058
Titre	Vulnérabilité dans SPIP
Date de la première version	08 février 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Secunia #SA18676 du 01 février 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

- Atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- SPIP versions 1.8.2-e et antérieures ;
- SPIP versions 1.9 Alpha 2 (5539).

3 Résumé

Une vulnérabilité dans SPIP permet à un utilisateur distant mal intentionné de porter atteinte à la confidentialité ou à l'intégrité des données du site web vulnérable.

4 Description

`SPIP` est un gestionnaire de contenu basé sur le langage `php`. Un manque de contrôle dans les paramètres `id_article` et `id_forum` du script `forum.php3` permettent à un utilisateur distant mal intentionné de

réaliser de l'injection de code SQL dans les requêtes effectuées par ce script. Il peut ainsi porter atteinte soit à la confidentialité soit à l'intégrité des données contenues dans la base de données adjointe à SPIP.

5 Solution

La vulnérabilité est corrigée dans la dernière version (snapshot 5546) disponible via Subversion (SVN).

6 Documentation

- Site de SPIP :
  http://www.spip.net
- Bulletin de sécurité Secunia :
  http://www.secunia.com/advisories/18676

Gestion détaillée du document

08 février 2006 version initiale.