



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 janvier 2009
N° CERTA-2008-AVI-612-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans SPIP

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-612>

Gestion du document

Référence	CERTA-2008-AVI-612-001
Titre	Vulnérabilités dans SPIP
Date de la première version	26 décembre 2008
Date de la dernière version	05 janvier 2009
Source(s)	Annonce de la version 2.02 de SPIP du 23 décembre 2008
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 SQL ;
- injection de code indirecte.

2 Systèmes affectés

- SPIP versions 2.0.1 et antérieures ;
- SPIP versions 1.9.2f et antérieures ;
- SPIP versions 1.8.3 et antérieures.

3 Résumé

Plusieurs vulnérabilités dans SPIP permettent d'exécuter du code arbitraire à distance, de réaliser des injections SQL et des attaques en *cross-site scripting*.

4 Description

Plusieurs vulnérabilités ont été corrigées dans *SPIP*. Leur exploitation permet d'exécuter du code arbitraire à distance, de réaliser des injections SQL et des attaques de type *cross-site scripting*.

5 Solution

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

6 Documentation

- Annonce de la version 2.02 de SPIP du 23 décembre 2008 :
<http://zine.spip.org/spip.php?article65>
- Référence CVE CVE-2008-5812 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5812>
- Référence CVE CVE-2008-5813 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5813>

Gestion détaillée du document

26 décembre 2008 version initiale.

05 janvier 2009 ajout des références CVE associées.