

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-2011-AVI-654>

Gestion du document

Référence	CERTA-2011-AVI-654
Titre	Vulnérabilités dans SPIP
Date de la première version	21 novembre 2011
Date de la dernière version	–
Source(s)	Annonce de SPIP du 17 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

- Élévation de privilèges ;
- injection de code indirecte à distance.

2 Systèmes affectés

- SPIP versions 1.9.x antérieures à 1.9.2n ;
- SPIP versions 2.0.x antérieures à 2.0.17 ;
- SPIP versions 2.1.x antérieures à 2.1.12.

3 Résumé

Des vulnérabilités dans SPIP permettent une élévation de privilèges dans l'application et une injection de code indirecte à distance.

4 Description

Plusieurs vulnérabilités ont été découvertes dans *SPIP* :

- un utilisateur authentifié peut élever ses privilèges au sein de *SPIP* et en devenir administrateur ;
- il est possible d’afficher le chemin d’installation ;
- une injection de code indirecte à distance est réalisable.

5 Solution

Les versions 1.9.2n, 2.0.17 et 2.1.12 corrigent ces vulnérabilités. La mise à jour de l’écran de sécurité (dernière version en date du 5 novembre 2011) est recommandée mais ne suffit pas pour les branches 2.0 et 2.1.

6 Documentation

- Annonce de SPIP du 17 novembre 2011 :
<http://archives.rezo.net/archives/spip-ann.mbox/2011/11/>

Gestion détaillée du document

21 novembre 2011 version initiale.