



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 octobre 2009  
N° CERTA-2009-AVI-466

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans CADIC Intégrale

---

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-2009-AVI-466>

---

### Gestion du document

Référence	CERTA-2009-AVI-466
Titre	Multiples vulnérabilités dans CADIC Intégrale
Date de la première version	30 octobre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité CADIC du 27 octobre 2009
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 ;
- contournement de la politique de sécurité ;
- injection de code indirecte.

## 2 Systèmes affectés

*CADIC Intégrale.*

## 3 Résumé

De multiples vulnérabilités dans *CADIC Intégrale* permettent, entre autres, d'exécuter du code arbitraire à distance.

## 4 Description

De multiples vulnérabilités ont été découvertes dans *CADIC Intégrale* :

- le téléchargement de fichier (*upload*) est possible, sans vérification du contrôle de celui-ci, ce qui permet d'exécuter du code arbitraire à distance ;

- certaines fonctionnalités sont accessibles à des profils non autorisés ;
- des injections SQL et des attaques de type *cross-site scripting* sont possibles via certains fichiers ;
- certains messages donnent trop d'informations.

## **5 Solution**

Des correctifs sont disponibles sur le site du club de *CADIC*.

## **6 Documentation**

- Bulletin de sécurité CADIC du 27 octobre 2009 :  
<http://club.cadic.fr/>

## **Gestion détaillée du document**

**30 octobre 2009** version initiale.