Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 octobre 2011
N° CERTA-2011-AVI-560

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Cadic Intégrale

Gestion du document

Référence	CERTA-2011-AVI-560
Titre	Vulnérabilités dans Cadic Intégrale
Date de la première version	12 octobre 2011
Date de la dernière version	–
Source(s)	Société Cadic
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 ;
- déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Cadic Intégrale versions 2007 (5.4.x), 2009 (5.5.x) et 2011.

3 Résumé

Trois vulnérabilités dans *Cadic Intégrale* permettent d'exécuter du code arbitraire à distance, de réaliser un déni de service ou de contourner le mécanisme d'authentification.

4 Description

Trois vulnérabilités ont été découvertes dans *Cadic Intégrale* :

- le serveur *Apache* installé est sensible au problème du traitement du paramètre `range` (CVE-2011-3192), ce qui permet de réaliser un déni de service à distance ;
- un composant fourni avec *Cadic Intégrale* permet le dépôt de fichiers. Il est ainsi possible de prendre le contrôle à distance du serveur ou d'exécuter du code arbitraire ;
- il est possible, dans une configuration très particulière, de contourner le mécanisme d'authentification.

5 Solution

Des correctifs sont disponibles auprès de l'éditeur ou via le site du club.

6 Documentation

- Site du Club Cadic :
  http://club.cadic.fr/
- Référence CVE CVE-2011-3192 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192

Gestion détaillée du document

12 octobre 2011 version initiale.