

Affaire suivie par :  
CERTA

## BULLETIN D'ALERTE DU CERTA

### Objet : Vulnérabilité d'ExtCalendar

---

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-2006-ALE-008>

---

### Gestion du document

Référence	CERTA-2006-ALE-008
Titre	Vulnérabilité d'ExtCalendar
Date de la première version	11 juillet 2006
Date de la dernière version	11 février 2013
Source(s)	
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.

## 2 Systèmes affectés

Les versions d'ExtCalendar antérieures ou égales à 2.0.

## 3 Résumé

Une vulnérabilité d'ExtCalendar permet à un utilisateur malveillant d'injecter du code arbitraire à distance.

## 4 Description

ExtCalendar est une application permettant de gérer un calendrier. Elle se présente comme un composant, qui peut être installé en association avec des CMS (pour *Content Management Systems*) de type Joomla! ou Mambo. Une vulnérabilité a été identifiée dans celle-ci. Elle ne vérifie pas correctement la variable `mosConfig_absolute_path`. Un utilisateur malveillant peut profiter de cette propriété pour injecter du code arbitraire à distance.

Cette vulnérabilité est actuellement exploitée.

## **5 Solution**

Ce produit n'est plus suivi par le CERTA.

## **6 Documentation**

Site du projet ExtCalendar :  
<http://extcal.sourceforge.net>

## **Gestion détaillée du document**

**11 juillet 2006** version initiale.