

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans WebCalendar

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-2012-AVI-230>

Gestion du document

Référence	CERTA-2012-AVI-230
Titre	Vulnérabilités dans WebCalendar
Date de la première version	24 avril 2012
Date de la dernière version	–
Source(s)	Révision CVS 1.168.2.1 du 28 février 2012
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

Versions antérieures à la 1.2.5.

3 Résumé

Deux vulnérabilités ont été corrigées dans *WebCalendar*. La première permet à un utilisateur non authentifié de réécrire le fichier « settings.php » avec des données arbitraires. La seconde est une « inclusion de fichier en local ». Toutes les deux peuvent mener à une « exécution de code arbitraire à distance ».

4 Solution

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

5 Documentation

- Révision CVS 1.168.2.1 du 28 février 2012 :
<http://webcalendar.cvs.sourceforge.net/viewvc/webcalendar/webcalendar/pref.php?revision=1.168.2.1&view=markup>
- Référence CVE CVE-2012-1495 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1495>
- Référence CVE CVE-2012-1496 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1496>

Gestion détaillée du document

24 avril 2012 version initiale.