



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 02 décembre 2009  
N° CERTA-2009-AVI-525

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans ActivePerl

---

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-525>

---

### Gestion du document

Référence	CERTA-2009-AVI-525
Titre	Multiples vulnérabilités dans ActivePerl
Date de la première version	02 décembre 2009
Date de la dernière version	–
Source(s)	Annonce de nouvelle version d'ActivePerl
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.

## 2 Systèmes affectés

ActivePerl versions antérieures à la version 5.10.1, mise à jour numéro 1006.

## 3 Résumé

Deux vulnérabilités ont été découvertes dans ActivePerl. L'exploitation de ces vulnérabilités permet de réaliser un déni de service à distance ou d'exécuter du code arbitraire à distance.

## 4 Description

Deux vulnérabilités ont été découvertes dans ActivePerl. Ces vulnérabilités, de type débordement de mémoire (*off-by-one*), affectent les bibliothèques de gestion de contenu compressé `Compress::Raw::Zlib` et `Compress::Raw::Zip2`. L'exploitation de ces vulnérabilités permet de réaliser un déni de service à distance ou d'exécuter du code arbitraire à distance.

## 5 Solution

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

## 6 Documentation

- Annonce de nouvelle version d'ActivePerl :  
<http://aspn.activestate.com/ASPN/Mail/Message/ActivePerl/3745416>
- Référence CVE CVE-2009-1391 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1391>
- Référence CVE CVE-2009-1884 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1884>

## Gestion détaillée du document

**02 décembre 2009** version initiale.