



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 27 mars 2007  
N° CERTA-2007-AVI-137-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de Zope

---

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-2007-AVI-137>

---

### Gestion du document

Référence	CERTA-2007-AVI-137-001
Titre	Vulnérabilité de Zope
Date de la première version	26 mars 2007
Date de la dernière version	27 mars 2007
Source(s)	Bulletin de sécurité Zope du 20 mars 2007
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

Élévation de privilèges.

## 2 Systèmes affectés

Logiciel *Zope*, jusqu'à la version 2.10.2.

## 3 Résumé

Une vulnérabilité de *Zope* de type *cross-site scripting* permet à un utilisateur malintentionné d'élever ses privilèges.

## 4 Description

Le logiciel *Zope* est un logiciel libre de développement de gestionnaires de contenu (CMS) et de portails.

Une vulnérabilité de type *cross-site scripting* permet à un utilisateur malveillant de modifier les paramètres de sécurité et/ou des comptes d'utilisateur. Cette vulnérabilité permet une élévation de privilèges.

## 5 Solution

Appliquer le correctif Hotfix-20070320. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

Noter que les versions 2.7 et antérieures ne sont plus maintenues. Le correctif n'a pas été testé pour ces versions.

## 6 Documentation

- Bulletin de sécurité *Zope* du 20 mars 2007 :  
<http://www.zope.org/Products/Zope/Hotfix-2007-03-20/announcement/view>
- Référence CVE CVE-2007-0240 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0240>

## Gestion détaillée du document

**26 mars 2007** version initiale.

**27 mars 2007** correction de la version affectée.