

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans CA XOsoft

---

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-2010-AVI-156>

---

### Gestion du document

Référence	CERTA-2010-AVI-156
Titre	Multiples vulnérabilités dans CA XOsoft
Date de la première version	07 avril 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité CA20100406-01 du 06 avril 2010
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 ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- CA XOsoft Replication r12.0 et r12.5 ;
- CA XOsoft High Availability r12.0 et r12.5 ;
- CA XOsoft Content Distribution r12.0 et r12.5.

## 3 Résumé

De multiples vulnérabilités dans CA XOsoft permettent d'exécuter du code arbitraire à distance et d'obtenir des données sensibles.

## 4 Description

De multiples vulnérabilités ont été découvertes dans *CA XOsoft* :

- un manque d'authentification permet à un attaquant de faire une requête SOAP afin d'obtenir les noms d'utilisateur (CVE-2010-1221);
- un problème similaire permet la récupération de données sensibles (CVE-2010-1222);
- de nombreux débordements de mémoire permettent l'exécution de code arbitraire à distance (CVE-2010-1223).

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité CA20100406-01 du 06 avril 2010 :  
<https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=232869>
- Référence CVE CVE-2010-1221 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1221>
- Référence CVE CVE-2010-1222 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1222>
- Référence CVE CVE-2010-1223 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1223>

## Gestion détaillée du document

**07 avril 2010** version initiale.