

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Symantec Altiris Notification Server

---

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-040>

---

### Gestion du document

Référence	CERTA-2010-AVI-040
Titre	Vulnérabilité dans Symantec Altiris Notification Server
Date de la première version	29 janvier 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Symantec SYM10-001 du 28 janvier 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 ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

*Symantec Altiris Notification Server* versions 6.0.x.

## 3 Résumé

Une vulnérabilité dans *Symantec Altiris Notification Server* permet de dévoiler des informations sur les machines du réseau et, dans certains cas, d'exécuter du code arbitraire à distance.

## 4 Description

Une clé statique, stockée sur le serveur *Symantec Altiris Notification Server*, est utilisée pour le chiffrement d'identifiants de connexion. Ces identifiants sont utilisés pour énumérer les machines d'un domaine sur lesquelles

un agent *Altiris* peut être déployé. De plus, si l'authentification à la base d'accès SQL repose sur des identifiants de connexion, une exécution de code arbitraire est possible. L'exploitation de cette vulnérabilité nécessite un accès à la console d'administration du serveur *Altiris*.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Symantec SYM10-001 du 28 janvier 2010 :  
[http://www.symantec.com/business/security\\_response/securityupdates/detail.jsp?fid=security\\_advisory&pvid=security\\_advisory&suid=20100128\\_00](http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&suid=20100128_00)
- Référence CVE CVE-2010-3035 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3035>

## Gestion détaillée du document

**29 janvier 2010** version initiale.