

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Symantec Altiris Deployment Solution

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-356>

Gestion du document

Référence	CERTA-2009-AVI-356
Titre	Multiples vulnérabilités dans Symantec Altiris Deployment Solution
Date de la première version	27 août 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Symantec SYM09-011 du 26 août 2009
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 ;
- élévation de privilèges.

2 Systèmes affectés

Symantec Altiris Deployment Solution versions 6.9.x.

3 Résumé

De multiples vulnérabilités dans *Symantec Altiris Deployment Solution* permettent, entre autres, d'exécuter du code arbitraire à distance.

4 Description

De multiples vulnérabilités ont été découvertes dans *Symantec Altiris Deployment Solution* :

- le système d'authentification de DBManager peut être contourné. Un attaquant peut ainsi modifier la base de données ;
- l'interface graphique d'AcClient fonctionne avec les privilèges de l'utilisateur connecté. Un utilisateur du groupe Everyone a des droits en écriture sur l'exécutable de cette interface. Il peut donc le remplacer par un autre exécutable, ce qui peut mener à une élévation des privilèges ;
- un utilisateur malintentionné contrôlant (ou simulant) un serveur *Altiris* peut envoyer des commandes à un client lors de la phase qui précède l'authentification ;
- un attaquant peut intercepter les fichiers envoyés par le serveur à un client légitime.

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 SYM09-011 du 26 août 2009 :

http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory\&pvid=security_advisory\&suid=20090826_00<http://www.symantec.com>

Gestion détaillée du document

27 août 2009 version initiale.