

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-2008-AVI-247>

Gestion du document

Référence	CERTA-2008-AVI-247
Titre	Multiples vulnérabilités dans Symantec Altiris Deployment Solution
Date de la première version	19 mai 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Symantec SYM008-012 du 15 mai 2008
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 ;
- contournement de la politique de sécurité ;
- élévation de privilèges.

2 Systèmes affectés

Symantec Altiris Deployment Solution versions 6.8.x et 6.9.x antérieures à 6.9.176.

3 Résumé

De multiples vulnérabilités ont été découvertes dans *Altiris Deployment Solution*, permettant notamment d'exécuter du code arbitraire à distance.

4 Description

Six vulnérabilités ont été découvertes dans *Symantec Altiris Deployment Solution* :

- une injection de commandes SQL est possible, ce qui conduit à une exécution de code arbitraire à distance ;
- une faille dans le chiffrement permet d'accéder à distance à des identifiants de domaine ;
- un utilisateur non privilégié peut, via son interface, accéder à un interpréteur de commandes ayant des privilèges élevés ;
- une vulnérabilité du même ordre que celle précédemment évoquée existe dans un élément de l'interface graphique (*tooltip*) ;
- un utilisateur peut modifier ou effacer les clés de registre créées par *Altiris Deployment Solution* ;
- un utilisateur ayant accès au répertoire d'installation d'*Altiris Deployment Solution* peut remplacer des composants de l'application et ainsi exécuter du code avec les privilèges de l'administrateur.

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 SYM008-012 du 15 mai 2008 :
<http://securityresponse.symantec.com/avcenter/security/Content/2008.05.14a.html>

Gestion détaillée du document

19 mai 2008 version initiale.