

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités d'EMC AlphaStor

---

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-273>

---

### Gestion du document

Référence	CERTA-2008-AVI-273
Titre	Vulnérabilités d'EMC AlphaStor
Date de la première version	28 mai 2008
Date de la dernière version	–
Source(s)	Bulletins de sécurité iDefense 702 et 703 du 27 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 ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

- EMC AlphaStor version 3.1 SP1 ainsi que celles antérieures.

## 3 Résumé

Des vulnérabilités ont été identifiées dans les applications de maintenance de disques EMC AlphaStor. Elles peuvent être exploitées par une personne malveillante distante afin d'exécuter du code arbitraire.

## 4 Description

- Des vulnérabilités ont été identifiées dans les applications de maintenance de disques EMC AlphaStor :
- certaines concernent le service *Server Agent* et en particulier le processus *Command Line Interface* en écoute par défaut sur le port 41025/tcp. Ces vulnérabilités peuvent être exploitées par une personne malveillante distante qui pourrait se connecter au port et envoyer une trame spécialement construite.

- une autre concerne le service `Library Manager` et en particulier le processus `robotd` en écoute par défaut sur le port 3500/tcp. Cette vulnérabilité peut être exploitée par une personne malveillante distante qui pourrait se connecter au port et envoyer une requête spécialement construite.

## 5 Solution

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

## 6 Documentation

- Site officiel EMC AlphaStor :  
<http://www.emc.com/products/detail/software/alphastor.htm>
- Base d'informations de EMC pour clients, article emc186391 :  
<http://powerlink.emc.com>
- Bulletin de sécurité iDefense 702 du 27 mai 2008 :  
<http://www.iddefense.com/ntelligence/vulnerabilities/display.php?id=702>
- Bulletin de sécurité iDefense 703 du 27 mai 2008 :  
<http://www.iddefense.com/ntelligence/vulnerabilities/display.php?id=703>
- Référence CVE CVE-2008-2157 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2157>
- Référence CVE CVE-2008-2158 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2158>

## Gestion détaillée du document

28 mai 2008 version initiale.