

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Symantec Enterprise Security Manager

---

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-2007-AVI-163>

---

### Gestion du document

Référence	CERTA-2007-AVI-163
Titre	Vulnérabilité dans Symantec Enterprise Security Manager
Date de la première version	10 avril 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Symantec SYM07-003 du 05 avril 2007
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.

## 2 Systèmes affectés

Toutes les versions de *Enterprise Security Manager* (ESM) antérieures à 6.5.3.

La version 6.5.3 n'est pas affectée par cette vulnérabilité. Les agents ESM sous NetWare 6.0, NetWare 6.5, OS/400 V5R2, OS/400V5R3, OpenVMS AXP 7.2 et OpenVMS AXP 7.3 ne sont pas affectés.

## 3 Résumé

Une vulnérabilité dans *Enterprise Security Manager* permet l'exécution de code arbitraire à distance.

## 4 Description

Une vulnérabilité a été découverte dans l'interface de mise à jour à distance de l'agent *Enterprise Security Manager* (ESM). L'agent ESM accepte des requêtes de toute entité capable d'interpréter le protocole de mise à jour. Un utilisateur malintentionné peut émuler le protocole de mise à jour pour exécuter du code arbitraire à distance sur les agents ESM.

## **5 Solution**

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).  
Le *manager* ESM, bien que non vulnérable, doit également être mis à jour pour interagir avec les agents.

## **6 Documentation**

- Bulletin de sécurité Symantec SYM07-003 du 05 avril 2007 :  
<http://securityresponse.symantec.com/avcenter/security/Content/2007.04.05d.html>

## **Gestion détaillée du document**

**10 avril 2007** version initiale.