Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 05 février 2008
N° CERTA-2008-AVI-047

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Symantec Backup Exec System Recovery Manager

Gestion du document

Référence	CERTA-2008-AVI-047
Titre	Vulnérabilité dans Symantec Backup Exec System Recovery Manager
Date de la première version	05 février 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Symantec SYM08-001 du 04 février 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

- Les versions de Symantec Backup Exec System Recovery Manager dans la branche 7.0 antérieures à 7.0.3.

3 Résumé

Une vulnérabilité a été identifiée dans *Symantec Backup Exec System Recovery Manager*. L'exploitation de cette dernière permettrait à une personne malveillante distante de télécharger n'importe où sur le serveur vulnérable tout fichier ou script.

4 Description

Une vulnérabilité a été identifiée dans *Symantec Backup Exec System Recovery Manager*. Elle concerne `FileUpdate Class` du serveur Apache Tomcat Symantec Livestate. Une personne malveillante pourrait émettre une requête

HTTP POST afin de télécharger n'importe où sur le serveur vulnérable un fichier ou un script. Cela lui permettrait donc d'exécuter du code à distance.

5 Solution

Se référer au bulletin de sécurité SYM08-001 de Symantec pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Document 297171 de Symantec relatif au bulletin SYM08-001 :
  http://seer.entsupport.com/docs/297171.htm
- Bulletin de sécurité Symantec SYM08-001 du 04 février 2008 :
  http://securityresponse.symantec.com/avcenter/security/Content/
- Référence CVE CVE-2008-0457 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0457

Gestion détaillée du document

05 février 2008 version initiale.