

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les gardes-barrières Symantec

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-2002-AVI-226>

Gestion du document

Référence	CERTA-2002-AVI-226
Titre	Vulnérabilité dans les gardes-barrières Symantec
Date de la première version	15 octobre 2002
Date de la dernière version	–
Source(s)	Bulletin Symantec
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

Déni de service

2 Systèmes affectés

- Raptor Firewall 6.5 (Windows NT) ;
- Raptor Firewall 6.5.3 (Solaris) ;
- Symantec Enterprise Firewall 6.5.2 (Windows NT et 2000) ;
- Symantec Enterprise Firewall 7.0 (Solaris) ;
- Symantec Enterprise Firewall 7.0 (Windows NT et 2000) ;
- VelociRaptor Model 500/700/1000 ;
- VelociRaptor Model 1100/1200/1300 ;
- Symantec Gateway Security 5110/5200/5300.

3 Résumé

Un utilisateur mal intentionné peut, par le biais de requêtes sur le serveur mandataire du garde-barrière, réaliser un déni de service sur ce dernier.

4 Description

Un utilisateur distant mal intentionné, ayant établi une connexion avec le serveur mandataire, peut par le biais de requêtes sur des liens hypertexte internes erronés ou inexistant, monopoliser toutes les ressources entraînant ainsi un déni de service.

5 Solution

Appliquer le correctif disponible sur le site Symantec (cf. section Documentation).

6 Documentation

Bulletin de sécurité Symantec

<http://securityresponse.symantec.com/avcenter/security/SymantecAdvisories.html>

Gestion détaillée du document

15 octobre 2002 version initiale.