Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 août 2004
N° CERTA-2004-AVI-280

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans divers produits Symantec

Gestion du document

Référence	CERTA-2004-AVI-280
Titre	Vulnérabilité dans divers produits Symantec
Date de la première version	30 août 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité SYM04-012 de Symantec du 26 août 2004
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.

2 Systèmes affectés

- Symantec Enterprise Firewall 8.0 (Windows et Solaris) ;
- Symantec Enterprise Firewall 7.0.x (Windows et Solaris) ;
- Symantec VelociRaptor 1.5 ;
- Symantec Gateway Security 1.0 - 5300 Series ;
- Symantec Gateway Security 2.0 - 5400 Series.

3 Résumé

Une vulnérabilité dans divers produits Symantec permet l'exécution de code arbitraire à distance, ou la réalisation d'un déni de service.

4 Description

La bibliothèque `Entrust LibKmp ISAKMP` gère l'échange des clés IKE et le traitement des paquets ISAKMP. Elle est utilisée par divers produits de sécurité de Symantec.

Une vulnérabilité de type débordement de mémoire affectant cette bibliothèque permet l'exécution de code arbitraire à distance ou la réalisation d'un déni de service.

Cette vulnérabilité n'affecte pas les passerelles qui n'utilisent que des tunnels VPN statiques ou qui n'ont pas de tunnels VPN dynamiques définis.

5 Solution

Appliquer le correctif fourni par Symantec :
http://www.symantec.com/region/fr/downloads

6 Documentation

- Bulletin de sécurité SYM04-012 de Symantec du 26 août 2004 :
  http://securityresponse.symantec.com/avcenter/security/Content/2004.08.26.html
- Référence CVE CAN-2004-0369 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0369

Gestion détaillée du document

30 août 2004 version initiale.