



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 septembre 2004
N° CERTA-2004-AVI-326

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans les pare-feux 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-2004-AVI-326>

Gestion du document

Référence	CERTA-2004-AVI-326
Titre	Multiples vulnérabilités dans les pare-feux Symantec
Date de la première version	24 septembre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité SYM04-013 de Symantec du 22 septembre 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

- Déni de service ;
- contournement des règles de filtrage pour l'interface Internet ;
- modification de la configuration du garde-barrière.

2 Systèmes affectés

- Symantec Firewall/VPN Appliance 100 en version du firmware antérieure à 1.63 ;
- Symantec Firewall/VPN Appliance 200/200R en version du firmware antérieure à 1.63 ;
- Symantec Gateway Security 320 en version du firmware antérieure à 622 ;
- Symantec Gateway Security 360/360R en version du firmware antérieure à 622.

3 Description

Trois vulnérabilités affectent certains produits Symantec.

La première permet de réaliser un déni de service en envoyant rapidement des paquets UDP sur tous les ports de l'interface Internet du pare-feu.

La seconde permet d'identifier les services UDP en envoyant des paquets ayant le port 53/udp en source sur l'interface Internet du pare-feu.

La troisième vulnérabilité concerne l'existence de noms de communauté SNMP par défaut qui ne peuvent être ni désactivés ni modifiés par l'interface d'administration. En exploitant la seconde vulnérabilité, il est possible d'envoyer des requêtes SNMP GET/SET.

4 Solution

Mettre le firmware à jour (version 1.63 pour Symantec Firewall/VPN Appliance et version 622 pour Symantec Gateway Security) :

<http://www.symantec.com/techsupp>

5 Documentation

Bulletin de sécurité SYM04-013 de Symantec du 22 septembre 2004 :

<http://securityresponse.symantec.com/avcenter/security/Content/2004.09.22.html>

Gestion détaillée du document

24 septembre 2004 version initiale.