Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 mai 2004
N° CERTA-2004-AVI-163

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans des produits de sécurité Symantec

Gestion du document

Référence	CERTA-2004-AVI-163
Titre	Multiples vulnérabilités dans des produits de sécurité Symantec
Date de la première version	13 mai 2004
Date de la dernière version	–
Source(s)	Avis de sécurité eEye AD20040512A Avis de sécurité eEye AD20040512B Avis de sécurité eEye AD20040512C Avis de sécurité eEye AD20040512D
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 ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

- Symantec Norton Internet Security 2002, 2003 et 2004 ;
- Symantec Norton Internet Security Professional 2002, 2003 et 2004 ;
- Symantec Norton Personal Firewall 2002, 2003 et 2004 ;
- Symantec Norton Antispam 2004 ;
- Symantec Client Firewall 5.01, 5.1.1 ;
- Symantec Client Security 1.0, 1.1, 2.0(SCF 7.1).

3 Résumé

Plusieurs vulnérabilités dans des produits de sécurité de la société Symantec permettent à un utilisateur mal intentionné de créer un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

Symantec intègre un pare-feu dans plusieurs produits de sécurité.
Quatre vulnérabilités ont été identifiées dans des fonctions du composant SYMDNS.sys :

- Deux vulnérabilités concernent une mauvaise gestion des paquets réponse NetBIOS Name Service (port source 137/UDP) permettant l'exécution de code arbitraire à distance ;
- deux vulnérabilités concernent une mauvaise gestion des paquets réponse DNS (port source 53/UDP) permettant la réalisation d'un déni de service ou l'exécution de code arbitraire à distance.

5 Solution

Appliquer les correctifs fournis par l'éditeur (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Symantec SYM04-008 du 12 mai 2004 :
  http://securityresponse.symantec.com/avcenter/security/Content/2004.05.12.html
- Bulletin de sécurité eEye AD20040512A du 12 mai 2004 :
  http://www.eeye.com/html/Research/Advisories/AD20040512A.html
- Bulletin de sécurité eEye AD20040512B du 12 mai 2004 :
  http://www.eeye.com/html/Research/Advisories/AD20040512B.html
- Bulletin de sécurité eEye AD20040512C du 12 mai 2004 :
  http://www.eeye.com/html/Research/Advisories/AD20040512C.html
- Bulletin de sécurité eEye AD20040512D du 12 mai 2004 :
  http://www.eeye.com/html/Research/Advisories/AD20040512D.html
- Référence CVE CAN-2004-0444 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0444
- Référence CVE CAN-2004-0445 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0445

Gestion détaillée du document

13 mai 2004 version initiale.