



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 février 2010
N° CERTA-2010-AVI-087-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans plusieurs produits 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-2010-AVI-087>

Gestion du document

Référence	CERTA-2010-AVI-087-001
Titre	Multiples vulnérabilités dans plusieurs produits Symantec
Date de la première version	22 février 2010
Date de la dernière version	23 février 2010
Source(s)	Bulletin de sécurité Symantec SYM10-002 du 17 février 2010 Bulletin de sécurité Symantec SYM10-003 du 17 février 2010 Bulletin de sécurité Symantec SYM10-004 du 17 février 2010
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

- Symantec AntiVirus versions 10.0.x, 10.1.x, et 10.2.x ;
- Norton Antivirus, SystemWorks, Confidential et Internet Security versions 2006, 2007 et 2008 ;
- Symantec Client Security versions 3.0.x, 3.1.x ;
- Symantec Endpoint Protection versions 11.x.

3 Résumé

De multiples vulnérabilités dans plusieurs produits *Symantec* permettent l'exécution de code arbitraire à distance ou le contournement de la politique de sécurité.

4 Description

De multiples vulnérabilités ont été découvertes dans plusieurs produits *Symantec* :

- une vulnérabilité de type débordement de mémoire a été découverte dans le composant *Symantec Client Proxy*. Un utilisateur peut exécuter du code arbitraire à distance par le biais d'un contrôle *ActiveX* spécialement conçu ;
- une vulnérabilité de type débordement de mémoire a été découverte dans la bibliothèque *SYMLTCOM.dll*. Un utilisateur peut l'exploiter pour exécuter du code arbitraire dans le contexte du navigateur de l'utilisateur ;
- une autre vulnérabilité concerne la fonctionnalité d'analyse antivirale à la demande. Cette analyse peut être contournée localement en effectuant un certain nombre d'actions spécifiques.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Symantec SYM10-002 du 17 février 2010 :
http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=2010&suid=20100217_00
- Bulletin de sécurité Symantec SYM10-003 du 17 février 2010 :
http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=2010&suid=20100217_01
- Bulletin de sécurité Symantec SYM10-004 du 17 février 2010 :
http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=2010&suid=20100217_02
- Référence CVE CVE-2010-0106 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0106>
- Référence CVE CVE-2010-0107 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0107>
- Référence CVE CVE-2010-0108 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0108>

Gestion détaillée du document

22 février 2010 version initiale.

23 février 2010 ajout d'une troisième vulnérabilité.