



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 août 2009
N° CERTA-2009-AVI-351

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les 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-2009-AVI-351>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2009-AVI-351 |
| Titre | Vulnérabilité dans les produits Symantec |
| Date de la première version | 26 août 2009 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Symantec SYM09-010 du 25 août 2009 |
| 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.

2 Systèmes affectés

- Symantec Mail Security for Domino versions 7.5.3.25, 7.5.4.29, 7.5.5.32, 7.5.6 et 8.0 ;
- Symantec Mail Security for Microsoft Exchange versions 5.0.10, 5.0.11, 5.0.12, 6.0.6, 6.0.7 et 6.0.8 ;
- Symantec Mail Security for SMTP versions 5.0.x ;
- Symantec Mail Security Appliance/Symantec BrightMail Appliance versions 5.0.x et ultérieures ;
- Symantec BrightMail Appliance versions 8.0.0 et 8.0.1 ;
- Symantec Data Loss Prevention Enforce/Detection Servers version 7.2 ;
- Symantec Data Loss Prevention Enforce/Detection Servers for Windows versions 8.1.1 et 9.0.1 ;
- Symantec Data Loss Prevention Enforce/Detection Servers for Linux versions 8.1.1 et 9.0.1 ;
- Symantec Data Loss Prevention Endpoint Agents versions 8.1.1 et 9.0.1.

3 Résumé

Une vulnérabilité dans des produits Symantec permet l'exécution de code arbitraire à distance.

4 Description

Une vulnérabilité a été découverte dans le module `Autonomy KeyView` fourni avec de nombreux produits *Symantec*. L'exploitation de cette vulnérabilité, par le biais d'un fichier au format `Excel`, permet l'exécution de code arbitraire à distance.

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 SYM09-010 du 25 août 2009 :

http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&suid=20090825_00

Gestion détaillée du document

26 août 2009 version initiale.