

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans des 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-111>

Gestion du document

Référence	CERTA-2010-AVI-111
Titre	Vulnérabilité dans des produits Symantec
Date de la première version	05 mars 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Symantec SYM10-006 du 04 mars 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.

2 Systèmes affectés

- Symantec Mail Security for Domino 8.0.2, 8.0.1, 8.0, 7.5.8, 7.5.7, 7.5.6, 7.5.5.32, 7.5.4.29, 7.5.3.25 ;
- Symantec Mail Security for Microsoft Exchange 6.0.9, 6.0.8, 6.0.7, 6.0.6, 5.0.13, 5.0.12, 5.0.11, 5.0.10 ;
- Symantec BrightMail Gateway 8.0.0, 8.0.1, 8.0.2 ;
- Symantec Mail Security for SMTP (EOL) 5.0.x ;
- Symantec Data Loss Prevention Enforce/Detection Servers 7.2 ;
- Symantec Data Loss Prevention Enforce/Detection Servers for Windows 8.1.1, 9.x, 10.0 ;
- Symantec Data Loss Prevention Enforce/Detection Servers for Linux 8.1.1, 9.x, 10.0 ;
- Symantec Data Loss Prevention Endpoint Agents 8.1.1 ;
- Symantec Data Loss Prevention Endpoint Agents 9.x ;
- Symantec Data Loss Prevention Endpoint Agents 10.0 ;
- Symantec IM Manager 2007 8.x.

3 Résumé

Une vulnérabilité dans un module tiers intégré dans certains produits Symantec, et concernant le traitement des documents utilisant la technologie OLE a été corrigée, et le module a été mis à jour.

4 Description

Une vulnérabilité dans le module tiers `Autonomy KeyView Filter`, intégré dans certains produits Symantec, et concernant le traitement des documents utilisant la technologie OLE, a été corrigée. La version à jour du module a été intégrée dans les dernières versions des produits Symantec.

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 SYM10-006 du 04 mars 2010 :
http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory
- Référence CVE CVE-2009-3032 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3032>

Gestion détaillée du document

05 mars 2010 version initiale.