



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 juillet 2010
N° CERTA-2010-AVI-339

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités 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-2010-AVI-339>

Gestion du document

Référence	CERTA-2010-AVI-339
Titre	Multiples vulnérabilités dans les produits Symantec
Date de la première version	28 juillet 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Symantec SYM10-009 du 27 juillet 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 ;
- déni de service à distance.

2 Systèmes affectés

- Symantec IM Manager 2007 8.x.
- Symantec Brightmail Gateway 9.x
- Symantec Mail Security for Domino 8.x ;
- Symantec Mail Security for Domino 7.x ;
- Symantec Mail Security for Microsoft Exchange 6.x ;
- Symantec Mail Security for SMTP 5.x ;
- Symantec Data Loss Prevention 8.x ;
- Symantec Data Loss Prevention Endpoint Agents 8.x ;
- Symantec Data Loss Prevention Endpoint Agents 10.x ;
- Symantec Data Loss Prevention Enforce/Detection Servers for-Linux 10.x ;
- Symantec Data Loss Prevention Enforce/Detection Servers for Windows 10.x ;

3 Résumé

Plusieurs vulnérabilités découvertes dans les produits Symantec permettent à un utilisateur distant malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

Plusieurs vulnérabilités de type débordement de mémoire dans les produits Symantec permettent à une personne malveillante de provoquer un déni de service ou d'exécuter du 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 SYM10-009 du 27 juillet 2010 :
http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory
- Référence CVE CVE-2010-0126 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0126>
- Référence CVE CVE-2010-0131 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0131>
- Référence CVE CVE-2010-0133 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0133>
- Référence CVE CVE-2010-0134 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0134>
- Référence CVE CVE-2010-0135 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0135>
- Référence CVE CVE-2010-1524 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1524>
- Référence CVE CVE-2010-1525 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1525>

Gestion détaillée du document

28 juillet 2010 version initiale.