

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-2011-AVI-582>

Gestion du document

Référence	CERTA-2011-AVI-582
Titre	Vulnérabilités dans plusieurs produits Symantec
Date de la première version	21 octobre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Symantec SYM11-013 du 06 octobre 2011
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 ;
- élévation de privilèges.

2 Systèmes affectés

- Symantec Mail Security for Microsoft Exchange versions 6.x ;
- Symantec Mail Security for Domino versions 7.5.x et 8.x ;
- Symantec Brightmail and Messaging Gateway versions 9.5 et antérieures ;
- Symantec Data Loss Prevention Enforce/Detection Servers versions 11.x, 10.x et antérieures ;
- Symantec Data Loss Prevention Endpoint Agents versions 11.x, 10.x et antérieures.

3 Résumé

Plusieurs vulnérabilités dans divers produits Symantec permettent à un utilisateur malintentionné, suivant le logiciel affecté, une élévation de privilège, un déni de service ou une exécution de code arbitraire à distance.

4 Description

Plusieurs vulnérabilités ont été découvertes dans Autonomy Verity Keyview Content Filter, fourni avec plusieurs logiciels Sysmantec. L'exploitation de ces vulnérabilités permet, en fonction du logiciel affecté, une élévation de privilège, un déni de service ou une 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 SYM11-013 du 06 octobre 2011 :
http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&suid=20111006_00
- Référence CVE CVE-2011-1512 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1512>
- Référence CVE CVE-2011-1213 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1213>
- Référence CVE CVE-2011-1214 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1214>
- Référence CVE CVE-2011-1215 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1215>
- Référence CVE CVE-2011-1216 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1216>
- Référence CVE CVE-2011-1518 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1518>
- Référence CVE CVE-2011-0337 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0337>
- Référence CVE CVE-2011-0338 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0338>
- Référence CVE CVE-2011-0339 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0339>

Gestion détaillée du document

21 octobre 2011 version initiale.