

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Symantec Message Filter

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-2012-AVI-355>

Gestion du document

Référence	CERTA-2012-AVI-355
Titre	Multiples vulnérabilités dans Symantec Message Filter
Date de la première version	28 juin 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Symantec du 28 juin 2012
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

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données ;
- injection de code indirecte à distance ;
- injection de requêtes illégitime par rebond.

2 Systèmes affectés

Versions antérieures à Symantec Message Filter 6.3 (correctif smf_630_p321).

3 Résumé

Quatre vulnérabilités ont été corrigées dans *Symantec Message Filter* :

- une permet d'accéder aux informations sur les changements de version des différents composants ;
- une permet de l'injection de code indirecte à distance (XSS) ;
- une concerne le vol de session d'un autre utilisateur ;
- la dernière est de type injection de requêtes illégitime par rebond (CSRF).

4 Solution

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

5 Documentation

- Bulletin de sécurité Symantec SYM12-010 du 26 juin 2012 :
http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=2012
- Référence CVE CVE-2012-0300 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0300>
- Référence CVE CVE-2012-0301 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0301>
- Référence CVE CVE-2012-0302 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0302>
- Référence CVE CVE-2012-0303 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0303>

Gestion détaillée du document

28 juin 2012 version initiale.