

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Symantec Messaging Gateway

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-468>

Gestion du document

Référence	CERTA-2012-AVI-468
Titre	Multiples vulnérabilités dans Symantec Messaging Gateway
Date de la première version	29 août 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Symantec SYM12-013 du 27 août 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

- Atteinte à la confidentialité des données ;
- élévation de privilèges ;
- injection de code indirecte à distance ;
- injection de requêtes illégitime par rebond.

2 Systèmes affectés

Symantec Messaging Gateway versions 9.5.x.

3 Résumé

Cinq vulnérabilités ont été corrigées dans la console de gestion de Symantec Messaging Gateway. Parmi celles-ci, une injection de code indirecte à distance (XSS), une injection de requêtes illégitime par rebond (CSRF), et un compte SSH avec un mot de passe par défaut permettant à un utilisateur illégitime d'avoir accès à la console, sont les plus critiques.

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 SYM12-013 du 27 août 2012 :
http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=2012&suid=20120827_00
- Référence CVE CVE-2012-0307 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0307>
- Référence CVE CVE-2012-0308 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0308>
- Référence CVE CVE-2012-3579 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3579>
- Référence CVE CVE-2012-3580 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3580>
- Référence CVE CVE-2012-3581 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3581>

Gestion détaillée du document

29 août 2012 version initiale.