

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Symantec Reporting Server

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-2007-AVI-250>

Gestion du document

Référence	CERTA-2007-AVI-250
Titre	Vulnérabilités dans Symantec Reporting Server
Date de la première version	06 juin 2007
Date de la dernière version	–
Source(s)	Bulletins de sécurité Symantec SYM-011 et SYM-012 du 05 juin 2007
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Symantec Reporting Server versions 1.0.197.0 et antérieures.

3 Résumé

Plusieurs vulnérabilités dans *Symantec Reporting Server* permettent d'avoir accès à la base de données de ce produit et, dans un cas très particulier, d'exécuter du code arbitraire à distance.

4 Description

Trois vulnérabilités ont été découvertes dans *Symantec Reporting Server*.

La première de ces vulnérabilités concerne une application Web optionnelle de la console de *Symantec System Center*. Un échec lors d'une tentative de connexion à *Reporting Server* peut entraîner l'affichage du condensé du

mot de passe de l'administrateur. Ce condensé peut être rejoué par un utilisateur malintentionné pour obtenir un accès à la base de données (référence CVE-2007-3022).

Une deuxième vulnérabilité permet de contourner le mécanisme d'authentification à la base de données de *Symantec Client Security Reporting Server* (référence CVE-2007-3022).

La troisième vulnérabilité est présente lors de la création d'un fichier par *Reporting Server*. Ce fichier peut être manipulé par un utilisateur malintentionné distant afin d'exécuter du code arbitraire à distance (référence CVE-2007-3021).

5 Solution

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

6 Documentation

- Bulletin de sécurité SYM-011 du 05 juin 2007 :
<http://www.symantec.com/avcenter/security/Content/2007.06.05.html>
- Bulletin de sécurité SYM-012 du 05 juin 2007 :
<http://www.symantec.com/avcenter/security/Content/2007.06.05a.html>
- Référence CVE CVE-2007-3021 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3021>
- Référence CVE CVE-2007-3022 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3022>

Gestion détaillée du document

06 juin 2007 version initiale.