

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Symantec Gateway Security

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-2004-AVI-063>

Gestion du document

Référence	CERTA-2004-AVI-063
Titre	Vulnérabilité dans Symantec Gateway Security
Date de la première version	03 mars 2004
Date de la dernière version	–
Source(s)	–
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 l'intégrité et à la confidentialité des données.

2 Systèmes affectés

Symantec Security Gateway 2.0.

3 Résumé

Une vulnérabilité de type `cross site scripting` affecte les boîtiers Symantec Gateway Security 2.0.

4 Description

Les boîtiers Symantec Gateway Security 2.0 (5400 Series) offrent des fonctionnalités de pare-feu, de détection d'intrusions, de filtrage d'adresses réticulaires, de filtre anti-spam...

Une vulnérabilité présente dans le traitement des adresses réticulaires par le serveur d'administration de Symantec Gateway Security 2.0 permet le vol de cookies. Un utilisateur mal intentionné peut ainsi voler le cookie `JSESSIONID` qui permet l'administration à distance du boîtier Symantec Gateway Security 2.0.

5 Solution

Appliquer le correctif SG8000-20040130-00 de l'éditeur :

http://www.symantec.com/techsupp/enterprise/products/sym_gateway_security/sym_gw_security_2_5400/files.html

6 Documentation

Note d'information CERTA-2002-INF-001 « Vulnérabilité de type Cross Site Scripting » :

<http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001/index.html>

Gestion détaillée du document

03 mars 2004 version initiale.