

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Symantec Ghost Solution Suite

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-2008-AVI-061>

Gestion du document

Référence	CERTA-2008-AVI-061
Titre	Symantec Ghost Solution Suite
Date de la première version	08 février 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Symantec SYM08-003 du 07 février 2008
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 Ghost Solution Suite, pour la version 1.1 ne disposant pas du patch 2 ;
- Symantec Ghost Solution Suite, pour les versions 2.0.0 et 2.0.1.

3 Résumé

Une vulnérabilité a été identifiée dans la suite d'administration de parcs informatiques Symantec Ghost Solution Suite. L'exploitation de cette dernière permettrait à une personne connectée au réseau interne, sous certaines conditions, d'exécuter des commandes arbitraires avec les droits administrateur (SYSTEM) sur les postes clients.

4 Description

Une vulnérabilité a été identifiée dans la suite d'administration de parcs informatiques *Symantec Ghost Solution Suite*. Elle concerne la méthode d'authentification établie entre la console de gestion Ghost et les clients *Ghost Management Agents* au niveau réseau (IP). L'exploitation de cette dernière permettrait à une personne connectée au réseau interne, sous certaines conditions, d'exécuter des commandes arbitraires avec les droits administrateur (SYSTEM) sur les postes clients.

5 Solution

Se référer au bulletin de sécurité SYM08-003 de Symantec pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Symantec SYM08-003 du 07 février 2008 :
<http://securityresponse.symantec.com/avcenter/security/Content/>
- Référence CVE CVE-2008-0640 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0640>

Gestion détaillée du document

08 février 2008 version initiale.