Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 24 mai 2012
N° CERTA-2012-AVI-291

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Symantec Endpoint Protection

Gestion du document

Référence	CERTA-2012-AVI-291
Titre	Vulnérabilités dans Symantec Endpoint Protection et Network Access Control
Date de la première version	24 mai 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Symantec SYM12-007 et SYM12-008 du 23 mai 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

- Exécution de code arbitraire à distance ;
- déni de service ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

- Pour la branche 11.x de Symantec Endpoint Protection, versions antérieures à la version 11 RU7 MP2 (11.0.720x) ;
- pour la branche 11.x de Symantec Endpoint Protection (Management Console), versions antérieures à la version 11 RU7 MP2 (11.0.720x) ;
- pour la branche 11.x de Symantec Network Access Control (Management Console), versions antérieures à la version 11 RU7 MP2 (11.0.720x) ;
- pour la branche 12.1.x de Symantec Endpoint Protection Manager, versions antérieures à la version 12 RU1 MP1 (12.1.110x).

3 Résumé

Plusieurs vulnérabilités ont été corrigées dans Symantec Endpoint protection.

Une vulnérabilité non détaillée par l'éditeur permet à un utilisateur malintentionné de provoquer un déni de service à distance (seule la version 11.x est affectée). Une deuxième vulnérabilité permettant une élévation de privilèges a été corrigée dans Symantec Endpoint Protection et Symantec Network Access Control (versions 11.x uniquement). Pour être exploitée, l'utilisateur malintentionné doit disposer d'un compte légitime sur le serveur. Une autre vulnérabilité concernant Symantec Endpoint Protection Manager 12.1.x a été corrigée. Elle permet à un utilisateur malintentionné d'exécuter du code arbitraire à distance et de porter atteinte à l'intégrité et à la confidentialité des données sur le serveur.

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 SYM12-007 du 23 mai 2012 :
  `http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&suid=20120522_00`
- Bulletin de sécurité Symantec SYM12-008 du 23 mai 2012 :
  `http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&suid=20120522_01`
- Référence CVE CVE-2012-1821 :
  `http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1821`
- Référence CVE CVE-2012-0289 :
  `http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0289`
- Référence CVE CVE-2012-0294 :
  `http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0294`
- Référence CVE CVE-2012-0295 :
  `http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0295`

Gestion détaillée du document

24 mai 2012 version initiale.