



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 18 février 2010  
N° CERTA-2010-AVI-086

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Cisco Security Agent

---

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-2010-AVI-086>

---

### Gestion du document

Référence	CERTA-2010-AVI-086
Titre	Multiples vulnérabilités dans Cisco Security Agent
Date de la première version	18 février 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco #111512 du 17 février 2010
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

- Déni de service à distance ;
- atteinte à la confidentialité des données ;
- injection de requêtes SQL.

## 2 Systèmes affectés

- Cisco Security Agent 5.1 ;
- Cisco Security Agent 5.2 ;
- Cisco Security Agent 6.0.

Remarque: seule la version 5.2 est affectée par la vulnérabilité de type déni de service.

## 3 Résumé

Plusieurs vulnérabilités sont présentes dans Cisco Security Agent. Celles-ci permettent de provoquer un déni de service à distance, de porter atteinte à la confidentialité des données ou de réaliser des injections SQL.

## 4 Description

Plusieurs vulnérabilités sont présentes dans les produits Cisco Security Agent :

- la première (CVE-2010-0146) concerne un problème de type traversée de répertoire et permet à un utilisateur authentifié malintentionné de porter atteinte à la confidentialité des données ;
- la seconde (CVE-2010-0147) permet à un utilisateur authentifié de conduire des attaques de type injection de requêtes SQL permettant la modification de la configuration de l'agent ;
- la dernière (CVE-2010-0148) permet à un utilisateur distant malintentionné de provoquer un déni de service de l'agent vulnérable par le biais de paquets TCP construits de façon particulière. Cette faille n'affecte pas les versions pour Windows et Sun Solaris.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Cisco 20100217-csa du 17 février 2010 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20100217-csa.shtml>
- Référence CVE CVE-2010-0146 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0146>
- Référence CVE CVE-2010-0147 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0147>
- Référence CVE CVE-2010-0148 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0148>

## Gestion détaillée du document

**18 février 2010** version initiale.