Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 octobre 2006
N° CERTA-2006-AVI-468

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

**Objet : Vulnérabilité dans Cisco Security Agent**



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2006-AVI-468 |
| Titre | Vulnérabilité dans Cisco Security Agent |
| Date de la première version | 26 octobre 2006 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Cisco ID 71902 du 25 octobre 2006 |
| 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.

## 2 Systèmes affectés

- Cisco Security Agent (CSA) 4.x pour GNU/Linux ;
- Cisco Security Agent (CSA) 5.x pour GNU/Linux ;
- Cisco Unified CallManager 5.x pour GNU/Linux ;
- Cisco Unified Presence Server pour GNU/Linux 1.x.

## 3 Résumé

Une vulnérabilité dans les produits `Cisco Security Agent` permet à un utilisateur malintentionné de provoquer un déni de service du système vulnérable.

# 4 Description

Une erreur dans la mise en œuvre de la détection de balayage de ports par `Cisco Security Agent` permet à un utilisateur distant de provoquer une consommation excessive de la mémoire du système `GNU/Linux` utilisant le `Security Agent` vulnérable. Cette vulnérabilité peut être utilisée par le biais d'un balayage de ports effectué de façon particulière.

# 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 ID 71902 du 25 octobre 2006 :
http://www.cisco.com/warp/public/707/cisco-sa-20061025-csa.shtml

# Gestion détaillée du document

**26 octobre 2006** version initiale.