Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 mai 2003
N° CERTA-2003-AVI-085

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du Service Assurance Agent (SAA) sous Cisco IOS

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-2003-AVI-085`

Gestion du document

Référence	CERTA-2003-AVI-085
Titre	Vulnérabilité du Service Assurance Agent (SAA) sous Cisco IOS
Date de la première version	16 mai 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco-sa-20030515-saa
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.

2 Systèmes affectés

Equipements Cisco utilisant certaines versions de Cisco IOS. Se référer au bulletin de sécurité de Cisco (cf. section Documentation) pour obtenir la liste des versions vulnérables.

3 Résumé

Au moyen de paquets RTR habilement constitués, un utilisateur mal intentionné peut forcer l'arrêt brutal d'un équipement Cisco utilisant une version vulnérable de Cisco IOS.

4 Description

SAA (Service Assurance Agent), anciennement RTR (Response Time Reporter), est un agent logiciel livré avec certaines versions de Cisco IOS sur des routeurs Cisco. Il permet de mesurer la disponibilité et les temps de réponse des équipements réseau.

Selon Cisco, une vulnérabilité présente dans le traitement de certains paquets RTR peut être exploitée par un utilisateur mal intentionné afin de forcer l'arrêt brutal du routeur Cisco.

La vulnérabilité ne peut être exploitée que si l'agent RTR est activé, ce qui n'est pas le cas par défaut. La commande "`show rtr responder`" permet de vérifier si l'agent est actif.

5 Contournement provisoire

L'agent RTR utilise le port `1967/udp`.

Il est conseillé de mettre en place sur les routeurs vulnérables un filtre permettant de rejeter les paquets en provenance de sources non sûres.

6 Solution

Contacter le constructeur pour l'obtention des correctifs.

7 Documentation

Bulletin de sécurité de Cisco :
http://www.cisco.com/warp/public/707/cisco-sa-20030515-saa.shtml

Gestion détaillée du document

16 mai 2003 version initiale.