Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 mai 2001
N° CERTA-2001-AVI-052

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du protocole HSRP sur les routeurs CISCO

Gestion du document

Référence	CERTA-2001-AVI-052
Titre	Vulnérabilité du protocole HSRP sur les routeurs CISCO
Date de la première version	14 mai 2001
Date de la dernière version	–
Source(s)	Documentation sur CISCO HSRP et IPSEC
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

Usurpation d'identité pouvant avoir pour conséquences un déni de service ou des « tempêtes » réseau.

2 Systèmes affectés

Tous les routeurs CISCO.

3 Résumé

Une vulnérabilité dans la gestion de l'authentification sous HSRP des routeurs CISCO permet à un utilisateur mal intentionné de falsifier l'identité d'un routeur CISCO. Cette vulnérabilité est connue depuis longtemps.

4 Description

Le protocole HSRP (*Hot Standby Routing Protocol*) est un protocole de routage implémenté dans les routeurs CISCO pour la gestion des liens de secours. HSRP sert à augmenter la tolérance de panne sur le réseau.

D'après CISCO, HSRP n'est pas un protocole sécurisé. Il n'est pas activé par défaut.

Dans ce protocole, la clé d'authentification des communications entre routeurs est diffusée en clair sur le réseau, et permet à une machine falsifiant l'adresse IP d'un des routeurs d'entraîner un mauvais routage des paquets et des conflits de priorité entre les routeurs.

Cette vulnérabilité permet entre autre chose d'effectuer un déni de service, ou une « tempête » sur le réseau. Des outils exploitants de cette vulnérabilité ont été diffusés sur l'Internet.

5 Contournement provisoire

- Filtrer le port 1985 en UDP pour les packets provenant de l'extérieur du réseau impliqué.
- CISCO propose d'installer IPSec entre les routeurs conformément au document cité dans le paragraphe documentation afin de chiffrer les communications HSRP et par conséquent la clé d'authentification.
- Utiliser un autre protocole : VRRP à la place de HSRP.

6 Solution

CISCO n'a pas l'intention de développer de correctif pour cette vulnérabilité.

7 Documentation

http://www.cisco.com/networkers/nw00/pres/2402.pdf

Gestion détaillée du document

14 mai 2001 version initiale.