Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 novembre 2001
N° CERTA-2001-AVI-147

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Corruption de cache ARP des équipements CISCO

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-2001-AVI-147

Gestion du document

Référence	CERTA-2001-AVI-147
Titre	Corruption de cache ARP des équipements CISCO
Date de la première version	22 novembre 2001
Date de la dernière version	–
Source(s)	Avis de sécurité CISCO
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

- Les routeurs CISCO des séries AGS/MGS/CGS/AGS+, IGS, RSM, 800, ubr900, 1000, 1400, 1500, 1600, 1700, 2500, 2600, 3000, 3600, 3800, 4000, 4500, 4700, AS5200, AS5300, AS5800, 6400, 7000, 7200, ubr7200, 7500, et 12000 ;
- les plus récentes versions de commutateurs ATM LS1010 ;
- les Catalyst 6000 ;
- les commutateurs de LAN Catalyst 2900XL ;
- les commutateurs de LAN des séries 1900, 2800, 2900, 3000, et 5000 ;
- et le DistributedDirector.

3 Résumé

Il est possible de corrompre les tables ARP de ces appareils avec des informations éronnées.

4 Description

Un paquet ARP destiné à une interface du routeur et contenant, pour l'adresse IP du routeur, une adresse MAC différente de la sienne, est censé être refusé. Mais au bout de plusieurs tentatives, pour éviter une « tempête », le routeur finira par accepter de remplacer sa propre adresse MAC par la nouvelle, rendant ainsi son interface inaccessible.

5 Contournement provisoire

Coder en dur l'adresse MAC de l'interface à protéger avec la commande suivante :

- Sous IOS :
  ```
  arp <adresse IP de l'interface> <adresse MAC de l'interface> <type>
  ```
- sous CatOS :
  ```
  set arp [dynamic|permanent|static] <adresse IP de l'interface> <adresse MAC
  de l'interface>
  ```

Cette commande n'est pas rémanente. Il faut la retaper après chaque redémarrage du routeur.

6 Solution

Selon les versions du système d'exploitation du routeur ou du commutateur, appliquer le correctif de CISCO ou mettre à jour la version du système comme indiqué dans le bulletin de sécurité de CISCO.

7 Documentation

Bulletin de sécurité CISCO :
http://www.cisco.com/warp/public/707/IOS-arp-overwrite-vuln-pub.shtml

Gestion détaillée du document

22 novembre 2001 version initiale.