Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 mai 2001
N° CERTA-2001-AVI-057

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans IOS version 12.1(2)T et 12.1(3)T

Gestion du document

Référence	CERTA-2001-AVI-057
Titre	Vulnérabilité dans IOS version 12.1(2)T et 12.1(3)T
Date de la première version	25 mai 2001
Date de la dernière version	–
Source(s)	Avis Cisco : "IOS Reload after Scanning Vulnerability"
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

Une exploitation de cette vulnérabilité permet de réaliser un déni de service.

2 Systèmes affectés

Tous les équipements Cisco utilisant les versions 12.1(2)T et 12.1(3)T de Cisco IOS.
Pour connaitre la version de Cisco IOS utilisée par un équipement, se connecter sur ce dernier et taper la commande suivante: `show version`

3 Résumé

Une tentative de connexion sur certaines plages de ports TCP entraine une erreur mémoire dans les équipements utilisant les versions 12.1(2)T et 12.1(3)T de Cisco IOS. Cette erreur entraine le redémarrage (`reload`) du logiciel.

4 Description

Une tentative de connexion sur des ports TCP entraine un erreur mémoire qui provoquera le redémarrage du logiciel lors de la prochaine utilisation d'une commande accédant au fichier de configuration comme par exemple `show running-config` ou `write memory`.

Les plages de ports TCP concernées sont:

- ports 3100 à 3999
- ports 5100 à 5999
- ports 7100 à 7999
- ports 10100 à 10999

Selon Cisco: « Cisco IOS ne peut être configuré pour supporter un service utilisant ces ports et ne peut être configuré pour accepter des connexions sur ces ports mais des tentatives de connexion provoquent une corruption de la mémoire qui pourra entrainer un rechargement du logiciel » .

5 Contournement provisoire

Il n'y a pas de solution de contournement provisoire.

Il est toutefois possible de protéger les équipements Cisco d'une attaque venant de l'extérieur au moyen d'un équipement (par exemple un pare-feu) filtrant les ports TCP concernés.

6 Solution

Télécharger une mise-à-jour du logiciel IOS sur le site de Cisco :
http://www.cisco.com

7 Documentation

Avis Cisco "IOS Reload after Scanning Vulnerability" :
http://www.cisco.com/warp/public/707/ios-tcp-scanner-reload-pub.shtml

Gestion détaillée du document

25 mai 2001 version initiale.