Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 juillet 2001
N° CERTA-2001-AVI-076

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

## Objet : Vulnérabilité dans PPTP sous CISCO IOS



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2001-AVI-076 |
| Titre | Vulnérabilité dans PPTP sous CISCO IOS |
| Date de la première version | 13 juillet 2001 |
| Date de la dernière version | – |
| Source(s) | Avis 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 entraînant l'arrêt du routeur Cisco.

## 2 Systèmes affectés

La vulnérabilité concerne tous les Cisco IOS qui acceptent le protocole PPTP. Les versions de Cisco IOS acceptant PPTP sont :

– 12.1 train, versions T, E, EZ, YA, YD et YC;
– 12.2 train, toutes les versions.

## 3 Résumé

Une vulnérabilité dans l'implémentation de PPTP sous Cisco IOS permet d'arrêter les routeurs Cisco à l'aide de paquets judicieusement composés.

# 4 Description

Le protocole PPTP (Point to Point Tunneling Protocol) permet à un utilisateur d'établir un tunnel vers un réseau IP (Internet Protocol) en utilisant le protocole PPP (Point to Point Protocol).

En envoyant un paquet judicieusement composé vers le port 1723/tcp (port de contrôle de PPTP), un utilisateur mal intentionné peut forcer l'arrêt du routeur.

Cette vulnérabilité ne nécessite pas de configuration particulière au niveau du routeur. Le routeur s'arrêtera au premier paquet reçu.

# 5 Solution

Télécharger les mises à jour sur le site de Cisco
http://www.cisco.com

# 6 Documentation

Avis de sécurité Cisco :
http://www.cisco.com/warp/public/707/PPTP-vulnerability-pub.html

# Gestion détaillée du document

**13 juillet 2001** version initiale.