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 septembre 2006
N° CERTA-2006-AVI-393

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans CISCO IOS

Gestion du document

Référence	CERTA-2006-AVI-393
Titre	Multiples vulnérabilités dans CISCO IOS
Date de la première version	14 septembre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité CISCO du 13 septembre 2006
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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

CISCO IOS version 12.x et versions inférieures disposant du VTP (VLAN Trunking Protocol)

3 Résumé

Plusieurs vulnérabilités, permettant l'exécution de code arbitraire à distance et/ou de provoquer un déni de service, ont été découvertes dans le module VTP (VLAN Trunking Protocol)

4 Description

Trois vulnérabilités ont été découvertes dans le module VTP de CISCO IOS :

- la première peut être exploitée par l'envoi de paquets malformés, afin de provoquer un déni de service ;

– la deuxième est due à une faille de type débordement d'espace mémoire, et peut être exploitée par un utilisateur mal intentionné afin d'exécuter du code arbitraire à distance sur l'équipement vulnérable ;
– la troisième vulnérabilité est présente au niveau de la validation des numéros de révision, ce qui pourrait être exploitée pour empêcher la mise à jour de l'équipement vulnérable.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

– Bulletin de sécurité Cisco ID 71306 du :
http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml

Gestion détaillée du document

14 septembre 2006 version initiale.