Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 avril 2006
N° CERTA-2006-AVI-167

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Plusieurs vulnérabilités dans Cisco IOS XR

Gestion du document

Référence	CERTA-2006-AVI-167
Titre	Plusieurs vulnérabilités dans Cisco IOS XR
Date de la première version	20 avril 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité de l'éditeur 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 à distance.

2 Systèmes affectés

Tout système fonctionnant sous Cisco IOS XR et configuré avec MPLS est affecté. Cette propriété est vérifiable sur le système Cisco par la commande `show mpls interfaces`, qui révèle les interfaces MPLS actives. Cisco IOS XR est installé dans certains produits CRS-1 et les séries 120000.

3 Résumé

Trois vulnérabilités dans l'implémentation MPLS du système d'exploitation Cisco IOS XR peuvent permettre à un utilisateur malveillant de provoquer un déni de service au niveau du routeur ciblé.

4 Description

Trois vulnérabilités existent dans l'implémentation MPLS du système d'exploitation Cisco XR, utilisé en particulier dans les routeurs de type Cisco CRS-1 ou dans la série 12000. MPLS (pour *Multi Protocol Label Switching*)

est un protocole de transport de données, fonctionnant au niveau de la couche de liaison du modèle OSI, et conçu pour encapsuler et véhiculer différents formats de paquets (Ethernet, Token Ring, ATM, Frame Relay, etc) au moyen de labels. Dans le cas où le système CISCO IOS XR est configuré avec MPLS, il est possible pour un utilisateur malveillant d'envoyer des paquets MPLS malformés. Ces derniers forcent le processus `NetIO` à redémarrer. Après plusieurs itérations, la carte réseau elle-même se relance, provoquant un déni de service pour les paquets devant être traîtés à ce moment-là.

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 69923 du 19 avril 2006 :
http://www.cisco.com/warp/public/707/cisco-sa-20060419-xr.shtml

Gestion détaillée du document

20 avril 2006 version initiale.