Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 juin 2004
N° CERTA-2004-AVI-203

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le traitement des paquets BGP par Cisco IOS

Gestion du document

Référence	CERTA-2004-AVI-203
Titre	Vulnérabilité dans le traitement des paquets BGP par Cisco IOS
Date de la première version	17 juin 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 53021
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

- Cisco IOS 11.x ;
- Cisco IOS 12.x ;
- Cisco IOS R11.x ;
- Cisco IOS R12.x.

3 Résumé

Une vulnérabilité dans le traitement des paquets BGP (`Border Gateway Protocol`) par Cisco IOS permet à une personne mal intentionnée de réaliser un déni de service sur l'équipement vulnérable.

4 Description

Le protocole BGP (`Border Gateway Protocol`) est un protocole de routage standard de l'Internet.

Une vulnérabilité présente dans le traitement des paquets BGP permet à une personne mal intentionnée, via l'envoi d'un paquet malicieusement construit, de rédémarrer les équipements configurés pour prendre en charge la gestion de BGP (par défaut, la gestion de ce protocole n'est pas activée).

Le paquet malicieusement construit doit avoir une adresse source appartenant à un pair (`peer`) de confiance.

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 53021 du 16 juin 2004 :
http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml

Gestion détaillée du document

17 juin 2004 version initiale.