Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 janvier 2005
N° CERTA-2005-AVI-030

Affaire suivie par :
CERTA

AVIS DU CERTA

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

Conditions d'utilisation de ce document : `http://www.certa.ssi.gouv.fr/certa/apropos.html`
Dernière version de ce document : `http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-030`

Gestion du document

Référence	CERTA-2005-AVI-030
Titre	Vulnérabilités dans le traitement des paquets BGP par Cisco IOS
Date de la première version	27 janvier 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco du 26 janvier 2005
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

L'ensemble des versions 9.x, 10.x, 11.x et 12.x sont affectées par ces vulnérabilités.

3 Résumé

Deux vulnérabilités sont présentent dans le traitement des paquets BGP (`Border Gateway Protocol`) par l'OS de Cisco (IOS), permettant à un utilisateur mal intentionné de réaliser un déni de service sur les équipements vulnérables.

4 Description

BGP (`Border Gateway Protocol`) est un protocole de routage standard de l'Internet (défini par la RFC 1771), utilisé pour l'interconnexion des AS (`Autonomous System`). Celui-ci n'est pas activé par défaut sur les routeurs Cisco.

Deux vulnérabilités affectent l'IOS des routeurs Cisco utilisant le routage BGP :

- Une vulnérabilité présente dans la gestion des paquets BGP par les routeurs Cisco permet à un individu mal intentionné, via l'envoi d'un paquet malicieusement construit, de redémarrer les équipements affectés suite à l'utilisation des commandes `show ip bgp neighbors` ou `debug ip bgp <neighbor> updates` par un administrateur ;
- L'envoi de paquets BGP malicieusement formés permet à un utilisateur mal intentionné de redémarrer les routeurs affectés et de les rendre inopérationnels pendant plusieurs minutes.

5 Solution

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

6 Documentation

Bulletin dé sécurité Cisco "Cisco IOS Misformed BGP Packet Causes Reload" du 26 janvier 2005 :
http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.pdf

Gestion détaillée du document

27 janvier 2005 version initiale.