

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans le routage BGP des équipements Cisco

---

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-2009-AVI-304>

---

### Gestion du document

Référence	CERTA-2009-AVI-304
Titre	Multiples vulnérabilités dans le routage BGP des équipements Cisco
Date de la première version	30 juillet 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco #110457 du 29 juillet 2009
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

- Cisco IOS 12.x ;
- Cisco IOS R12.x ;
- Cisco IOS XE 2.3.x ;
- Cisco IOS XE 2.4.x.

## 3 Résumé

Plusieurs vulnérabilités relatives au routage BGP présentes dans les équipements Cisco permettent à un utilisateur distant de provoquer un déni de service.

## 4 Description

Deux vulnérabilités relatives au routage BGP sont présentes dans certains équipements Cisco :

- la première concerne le traitement de certaines requêtes de mise à jour (*update*) incluant un chemin d'accès d'AS (Autonomous System) particulier ;
- la seconde, de nature non-précisée par le constructeur, est également relative à la gestion des messages de type *update*.

Toutes deux permettent à un utilisateur distant malintentionné de provoquer un déni de service par le biais de requêtes BGP particulières.

## 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 20090729-bgp du 29 juillet 2009 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20090729-bgp.shtml>
- Référence CVE CVE-2009-1168 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1168>
- Référence CVE CVE-2009-2049 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2049>

## Gestion détaillée du document

30 juillet 2009 version initiale.