

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Cisco IOS XR

---

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-2010-AVI-410>

---

### Gestion du document

Référence	CERTA-2010-AVI-410
Titre	Vulnérabilité dans Cisco IOS XR
Date de la première version	30 août 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 20100827-bgp du 29 août 2010
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

Tous les matériels avec le logiciel *Cisco IOS XR* configuré pour le routage BGP.

## 3 Résumé

Une vulnérabilité dans *Cisco IOS XR* permet de réaliser un déni de service à distance.

## 4 Description

Une vulnérabilité a été découverte dans la gestion des préfixes BGP par *Cisco IOS XR*. Un appareil utilisant *Cisco IOS XR*, qui reçoit un préfixe BGP avec un attribut transitif spécifique, va corrompre cet attribut avant de le réémettre à ses voisins. Les voisins peuvent alors réinitialiser la session BGP.

## **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 20100827-bgp du 29 août 2010 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20100827-bgp.shtml>
- Référence CVE CVE-2010-3035 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3035>

## **Gestion détaillée du document**

**30 août 2010** version initiale.