

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de 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-2009-AVI-344>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2009-AVI-344 |
| Titre | Vulnérabilités de Cisco IOS XR |
| Date de la première version | 21 août 2009 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Cisco cisci-sa-20090818-bgp du 18 août 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 XR avec gestion du routage BGP activée.

3 Résumé

Plusieurs vulnérabilités affectent le traitement BGP de Cisco IOS XR et permettent à un utilisateur malveillant de provoquer un déni de service à distance.

4 Description

Plusieurs vulnérabilités affectent le traitement BGP de Cisco IOS XR :

- le traitement défectueux d'un message BGP anormalement long de mise à jour de routage provoque un arrêt inopiné du processus BGP. Ce défaut permet à un utilisateur malveillant de provoquer un déni de service à distance ;

- le traitement défectueux d'un message BGP de mise à jour de routage malformé provoque un arrêt de la négociation BGP. Ce défaut permet à un utilisateur malveillant de provoquer un déni de service à distance ;
- le traitement défectueux d'un message BGP de mise à jour de routage avec un nombre élevé d'AS provoque un arrêt inopiné du processus BGP. Ce défaut permet à un utilisateur malveillant de provoquer un déni de service à distance.

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 20090818-bgp du 18 août 2009 :
<http://www.cisco.com/warp/public/707/cisco-sa-20090818-bgp.shtml>
- Référence CVE CVE-2009-1154 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1154>
- Référence CVE CVE-2009-2055 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2055>
- Référence CVE CVE-2009-2056 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2056>

Gestion détaillée du document

21 août 2009 version initiale.