

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité Cisco IOS aux dénis de service de type ICMP Redirect

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-2002-AVI-107>

Gestion du document

Référence	CERTA-2002-AVI-107
Titre	Vulnérabilité Cisco IOS aux dénis de service de type ICMP Redirect
Date de la première version	23 mai 2002
Date de la dernière version	–
Source(s)	Bulletin de securite Bugtraq
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

Certaines versions de Cisco IOS 11.X et 12.X.

Matériels connus comme vulnérables :

- Cisco 1005 IOS 11.0(18) ;
- Cisco 1603 IOS 11.3(11b) ;
- Cisco 1603 IOS 12.0(3) ;
- Cisco 2503 IOS 11.0(22a) ;
- Cisco 2503 IOS 11.1(24a).

3 Résumé

Certaines versions de l'IOS (Internetwork Operating System) des matériels de CISCO sont vulnérables aux attaques par déni de service de type ICMP Redirect.

4 Description

Les messages ICMP Redirect sont utilisés dans les réseaux de type IP afin de modifier dynamiquement les tables de routage d'un équipement réseau (annonce de nouvelles routes). Certaines versions d'IOS possèdent une mauvaise gestion de ce type de messages. Cette vulnérabilité peut être exploitée par un individu mal intentionné afin d'effectuer un déni de service sur les routeurs vulnérables.

5 Contournement provisoire

Il est possible d'interdire les messages de type ICMP Redirect à destination du routeur vulnérable, s'ils ne sont pas utilisés.

```
access-list 101 deny icmp any host <adresse routeur> redirect
```

6 Solution

Contactez CISCO afin d'obtenir le correctif.

7 Documentation

Bulletin de sécurité Bugtraq :
<http://online.securityfocus.com/bid4786/discussion>

Gestion détaillée du document

23 mai 2002 version initiale.