

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité du serveur HTTP dans 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-2003-AVI-129>

---

### Gestion du document

Référence	CERTA-2003-AVI-129
Titre	Vulnérabilité du serveur HTTP dans CISCO IOS
Date de la première version	31 juillet 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité CISCO
Pièce(s) jointe(s)	Aucune

Une gestion de version détaillée se trouve à la fin de ce document.

## 1 Risque

- Exécution de code arbitraire à distance
- Déni de service

## 2 Systèmes affectés

Tout système fonctionnant sous CISCO IOS, sauf les versions 12.3 et 12.3T.

## 3 Résumé

Le serveur HTTP des systèmes CISCO IOS peut être activé si spécifié dans la configuration. Une vulnérabilité de type débordement de mémoire dans le code permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire sur le système.

## 4 Description

Une requête standard GET du protocole HTTP volontairement mal formée permet d'exploiter la vulnérabilité.

## **5 Contournement provisoire**

Limiter les hôtes ou réseaux autorisés à se connecter au serveur HTTP en créant des “access lists” adéquates.

## **6 Solution**

Se référer au bulletin de sécurité Cisco (cf. section Documentation) pour l’obtention d’un correctif.

## **7 Documentation**

Bulletin de sécurité CISCO (“Sending 2GB Data in GET Request Causes Buffer Overflow in Cisco IOS Software”):

<http://www.cisco.com/warp/public/707/cisco-sn-20030730-ios-2gb-get.shtml>

## **Gestion détaillée du document**

**31 juillet 2003** version initiale.