

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du serveur TFTP 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-2002-AVI-161>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2002-AVI-161 |
| Titre | Vulnérabilité du serveur TFTP dans CISCO IOS |
| Date de la première version | 31 juillet 2002 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité CISCO |
| 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

Cisco IOS versions 11.1, 11.2, 11.3.

Les équipements équipés d'une architecture basée sur un processeur de type 68040 ne sont pas affectés. La commande `show version` tapée au prompt du routeur permet de vérifier cette information.

3 Résumé

Le serveur TFTP fourni dans certaines versions de Cisco IOS est vulnérable à un débordement de mémoire.

4 Description

Le protocole TFTP (Trivial File Transfert Protocol) permet de transférer facilement des fichiers entre ou sur les équipements réseaux. Une vulnérabilité présente dans le serveur TFTP de certaines versions de Cisco IOS permet à un utilisateur mal intentionné d'effectuer un déni de service par l'envoi d'une requête malicieusement construite.

5 Contournement provisoire

Désactiver le serveur TFTP.

6 Documentation

Bulletin de sécurité CISCO "TFTP Long Filename Vulnerability" :
<http://www.cisco.com/warp/public/707/ios-tftp-long-filename-pub.shtml>

Gestion détaillée du document

31 juillet 2002 version initiale.