

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-128>

Gestion du document

Référence	CERTA-2003-AVI-128
Titre	Vulnérabilité dans CISCO IOS
Date de la première version	31 juillet 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité CISCO "Enumerating Locally Defined Users in CISCO IOS"
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

Divulgateion d'informations.

2 Systèmes affectés

– CISCO IOS 11.X

Les systèmes utilisant le service d'authentification AAA `new-model` ne sont pas concernés.

3 Résumé

Une vulnérabilité a été découverte dans l'IOS de Cisco permettant à un individu mal intentionné de lister les utilisateurs définis localement.

4 Description

Un utilisateur mal intentionné peut déterminer la liste des utilisateurs définis localement en analysant les messages id'erreur renvoyés lors d'une authentification sur le routeur via Telnet.

5 Solution provisoire

Désactiver Telnet et utiliser SSH ou bien l'authentification de type AAA `new-model`.

6 Documentation

Bulletin de sécurité CISCO "Enumerating Locally Defined Users in CISCO IOS":
<http://www.cisco.com/warp/public/707/cisco-sn-20030724-ios-enum.shtml>

Gestion détaillée du document

31 juillet 2003 version initiale.