

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Cisco Aironet

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-074>

Gestion du document

Référence	CERTA-2002-AVI-074
Titre	Vulnérabilité de Cisco Aironet
Date de la première version	10 avril 2002
Date de la dernière version	–
Source(s)	Avis 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

Toutes les versions de Cisco Aironet à l'exception de la 11.21.
Sont également affectés les matériels suivants :

- Cisco Aironet Access Point 340 et 350 ;
- Cisco Aironet Bridge 350.

3 Résumé

Un utilisateur mal intentionné peut exploiter une vulnérabilité de l'accès Telnet pour provoquer un déni de service.

4 Description

Si l'accès Telnet est activé sur l'un des produits cités ci-dessus, et si un mot de passe est demandé pour l'authentification, il est alors possible de faire redémarrer le système.

5 Contournement provisoire

Désactiver l'accès Telnet.

6 Solution

Installer la version 11.21 du logiciel.

7 Documentation

Avis de sécurité Cisco :

<http://www.cisco.com/warp/public/707/Aironet-Telnet.shtml>

Gestion détaillée du document

10 avril 2002 version initiale.