Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 12 juillet 2001
N° CERTA-2001-AVI-074

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans les Cisco VN 5420

Gestion du document

Référence	CERTA-2001-AVI-074
Titre	Vulnérabilités dans les Cisco VN 5420
Date de la première version	12 juillet 2001
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 ;
- Accès au shell développeur.

2 Systèmes affectés

Cisco SN 420 Storage Routeurs utilisant une version logicielle inférieure ou égale à 1.1(3).

3 Résumé

Une utilisateur distant mal intentionné peut, par le biais de différentes requêtes sur le port 8023, soit entraîner un redémarrage du Cisco ou soit avoir accès au shell développeur.

4 Description

- Première vulnérabilité :
  Une succesion rapide de connexions sur le port TCP 8023 déclenche un déni de service sur le Cisco SN 420, entraînant un redémarrage du routeur.

– Seconde vulnérabilité :
  Un accès « rlogin » effectué sur le port 8023 à partir du GigabitEthernet (carte de connexion haut débit des routeurs Cisco) ou directement sur l'interface d'administration permet d'avoir accès au shell développeur sans mot de passe.

5 Solution

Télécharger la version 1.1(4) sur le site CISCO :
http://www.cisco.com

6 Documentation

Bulletin de sécurité CISCO :
http://www.cisco.com/warp/public/707/SN-kernel-pub.html

Gestion détaillée du document

12 juillet 2001 version initiale.