



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 16 décembre 2003  
N° CERTA-2003-AVI-213

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de Cisco ACNS

---

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-213>

---

### Gestion du document

|                             |                             |
|-----------------------------|-----------------------------|
| Référence                   | CERTA-2003-AVI-213          |
| Titre                       | Vulnérabilité de Cisco ACNS |
| Date de la première version | 16 décembre 2003            |
| 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 ;
- exécution de code arbitraire à distance.

## 2 Systèmes affectés

- Cisco ACNS versions 4.2.10 et antérieures ;
- Cisco ACNS versions 5.0.4 et antérieures.

Les produits affectés sont les suivants :

- Content Routers séries 4400 ;
- Content Distribution Manager séries 4600 ;
- Content Engine séries 500 et 7300 ;
- Content Engine Module for Cisco Routers séries 2600, 3600 et 3700.

### **3 Résumé**

Une vulnérabilité dans le module d'authentification du logiciel Cisco ACNS (Application and Content Networking System) permet à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

### **4 Description**

Une vulnérabilité dans le module d'authentification du logiciel Cisco ACNS permet à un utilisateur mal intentionné d'arrêter le système ou de prendre à distance le contrôle du système, en entrant un mot de passe particulièrement long.

### **5 Contournement provisoire**

Désactiver l'interface graphique du serveur (GUI): `no gui-server enable`

### **6 Solution**

Se référer au bulletin de sécurité du constructeur (cf. section Documentation) pour l'obtention des correctifs.

### **7 Documentation**

Bulletin de sécurité de Cisco :  
<http://www.cisco.com/warp/public/707/cisco-sa-20031210-ACNS-auth.shtml>

### **Gestion détaillée du document**

16 décembre 2003 version initiale.