

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités du système 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-2005-AVI-090>

Gestion du document

Référence	CERTA-2005-AVI-090
Titre	Vulnérabilités du système Cisco ACNS
Date de la première version	28 février 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco #64069 du 24 février 2005
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 ;
- élévation de privilèges.

2 Systèmes affectés

Système Cisco ACNS versions 4.X, 5.0, 5.1 et 5.2.

Voici la liste des plates-formes supportant le service ACNS :

- Cisco Content Engines 500 et 7300 ;
- Cisco Content Routers 4400 ;
- Cisco Content Distribution Manager 4600 ;
- Cisco Content Engine Module pour Cisco 2600, 2800, 3600, 3700 et 3800 (Integrated Service Routers).

Se reporter au bulletin de sécurité Cisco pour connaître quelles versions du système ACNS sont précisément vulnérables en fonction de chaque vulnérabilité.

3 Résumé

Quatre vulnérabilités découvertes dans le système Cisco ACNS peuvent être exploitées pour provoquer un déni de service.

De plus, un mot de passe est activé par défaut pour le compte administrateur.

4 Description

Le système Cisco ACNS (*Application and Content Networking System*) est utilisé pour la diffusion de données et d'applications Web.

- Vulnérabilité CSCef27476 : un utilisateur mal intentionné peut provoquer le redémarrage du processus du cache ACNS par le biais de paquets TCP malicieusement construits.
- Vulnérabilité CSCef30460 : un utilisateur mal intentionné peut provoquer une saturation des ressources par le biais de paquets IP malicieusement construits.
- Vulnérabilité CSCeg49648 : cette vulnérabilité concerne le service «*RealServer Real Subscriber*» et permet à un utilisateur mal intentionné de provoquer une saturation des ressources par le biais de paquets IP malicieusement construits. Par défaut, le service «*RealServer Real Subscriber*» n'est pas activé.
- Vulnérabilité CSCeg23731 : cette vulnérabilité concerne la gestion des paquets IP et permet à un utilisateur mal intentionné de provoquer un déni de service.
- Vulnérabilité CSCef30743 : un mot de passe par défaut est activé pour le compte administrateur sur le produit ACNS.

5 Contournement provisoire

Vulnérabilité CSCef30743 : modifier le mot de passe par défaut.

6 Solution

Se référer au bulletin de sécurité pour obtenir les correctifs (cf. section Documentation).

7 Documentation

Bulletin de sécurité Cisco #64069 du 24 février 2005 :
<http://www.cisco.com/warp/public/707/cisco-sa-20050224-acnsdos.shtml>

Gestion détaillée du document

28 février 2005 version initiale.