Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 avril 2008
N° CERTA-2008-AVI-210

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Cisco NAC Appliance

Gestion du document

Référence	CERTA-2008-AVI-210
Titre	Vulnérabilité dans Cisco NAC Appliance
Date de la première version	17 avril 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 100782 publié le 16 avril 2008
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

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Cisco NAC Appliance pour les versions de la branche 3.5.x ;
- Cisco NAC Appliance pour les versions de la branche 3.6.x antérieures à 3.6.4.4 ;
- Cisco NAC Appliance pour les versions de la branche 4.0.x antérieures à 4.0.6 ;
- Cisco NAC Appliance pour les versions de la branche 4.1.x antérieures à 4.1.2.

3 Résumé

Une vulnérabilité a été identifiée dans Cisco NAC (*Network Admission Control*) Appliance. Elle permettrait à une personne malveillante distante de récupérer des informations pour contourner la politique de sécurité et de prendre le contrôle de certains éléments servant à la mettre en place.

4 Description

Une vulnérabilité a été identifiée dans Cisco NAC (*Network Admission Control*) Appliance. Elle permettrait à une personne malveillante distante de récupérer via les journaux d'erreurs transmis dans le réseau un secret partagé entre les éléments de type CAS (*Cisco Clean Access Server*) et CAM (*Cisco Clean Access Manager*).

Cette exploitation peut donc conduire non seulement au contournement de la politique de sécurité appliquée, mais également au contrôle complet du CAS.

5 Solution

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

6 Documentation

- Bulletin de sécurité Cisco 20080416-nac du 16 avril 2008 :
  http://www.cisco.com/warp/public/707/cisco-sa-20080416-nac.shtml
- Référence CVE CVE-2008-1155 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1155

Gestion détaillée du document

17 avril 2008 version initiale.