Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 31 août 2005
N° CERTA-2005-AVI-317-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Cisco Clean Access

Gestion du document

Référence	CERTA-2005-AVI-317-001
Titre	Vulnérabilité dans Cisco Clean Access
Date de la première version	18 août 2005
Date de la dernière version	31 août 2005
Source(s)	Bulletin de sécurité Cisco 66068 du 17 août 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 ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Cisco Clean Access versions 3.3.0 à 3.3.9 ;
- Cisco Clean Access versions 3.4.0 à 3.4.5 ;
- Cisco Clean Access versions 3.5.0 à 3.5.3.

3 Résumé

Une vulnérabilité dans `Cisco Clean Access` permet à un utilisateur mal intentionné du réseau local de provoquer un déni de service, de contourner la politique de sécurité ou de porter atteinte à la confidentialité des données.

4 Description

`Cisco Clean Access` est une solution logicielle permettant de gérer les accès des machines au réseau local. Elle comprend une `API` (`Application Program Interface`) donnant accès à différentes fonctionnalités.

Un manque de contrôle dans l'utilisation de ces fonctionnalités permet à un utilisateur mal intentionné du réseau local, par le biais d'un script malicieusement construit, de provoquer un déni de service en ajoutant une machine cible dans la liste des machines à rejeter. Elle permet également de contourner la politique de sécurité en ajoutant une machine arbitraire dans la liste des machines de confiance. Elle permet enfin d'atteindre à la confidentialité des données disponibles dans la configuration de `Cisco Clean Access`.

5 Solution

Se référer au bulletin de sécurité Cisco pour appliquer le correctif approprié (cf. Documentation).

6 Documentation

- Bulletin de sécurité Cisco 66068 du 17 août 2005 :
  http://www.cisco.com/warp/public/707/cisco-sa-20050817-cca.shtml
- Bulletin de sécurité Cisco 66147 du 22 août 2005 :
  http://www.cisco.com/warp/public/707/cisco-sa-20050822-cca.shtml

Gestion détaillée du document

18 août 2005 version initiale.
31 août 2005 ajout de la référence au bulletin de sécurité Cisco #66147.