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 mai 2006
N° CERTA-2006-AVI-201

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Cisco AVS

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-2006-AVI-201

Gestion du document

Référence	CERTA-2006-AVI-201
Titre	Vulnérabilité dans Cisco AVS
Date de la première version	16 mai 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité CISCO 20060510-avs
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.

2 Systèmes affectés

- AVS 3110 versions 4.0 et 5.0 ;
- AVS 3120 version 5.0.0.

3 Résumé

Une vulnérabilité présente sur Cisco `AVS (Application Velocity System's)` peut être exploitée par un utilisateur mal intentionné pour contourner la politique de sécurité via une requête HTTP malicieusement construite.

4 Description

Une vulnérabilité est présente dans la configuration par défaut de `Cisco AVS`. Un utilisateur mal intentionné peut exploiter, via une requête HTTP malveillante, le système vulnérable et l'utiliser comme serveur mandataire

(proxy) transparent pour accéder à des ports de destination arbitraires.
Un changement dans la configuration par défaut permet de ne plus être vulnérable.

La version 5.0.1 n'est pas impactée par cette vulnérabilité.

5 Solution

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

6 Documentation

- Bulletin de sécurité Cisco ID 20060510-avs du 10 mai 2006 :
  http://www.cisco.com/warp/public/707/cisco-sa-20060510-avs.shtml

Gestion détaillée du document

16 mai 2006 version initiale.