



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 septembre 2006
N° CERTA-2006-AVI-403

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité CISCO IOS

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-403>

Gestion du document

Référence	CERTA-2006-AVI-403
Titre	Vulnérabilité CISCO IOS
Date de la première version	21 septembre 2006
Date de la dernière version	–
Source(s)	
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

- CISCO IAD2430 Integrated Access Device ;
- CISCO IAD2431 Integrated Access Device ;
- CISCO IAD2432 Integrated Access Device ;
- CISCO VG224 Analog Phone Gateway ;
- CISCO MWR 1941 Mobile Wireless Edge Router ;
- CISCO MWR 1900 Mobile Wireless Edge Router ;
- CISCO IOS 12.2 ;
- CISCO IOS 12.3 ;
- CISCO IOS 12.4.

3 Résumé

Une vulnérabilité dans CISCO IOS a été découverte et permet à des agresseurs distants de compromettre un système vulnérable.

4 Description

La vulnérabilité concerne le service SNMP qui devient accessible en lecture et écriture du fait de la nécessaire compatibilité avec la spécification Data Over Cable Service Interface Specification (DOCSIS). La vulnérabilité permet de prendre le contrôle d'un système vulnérable.

5 Solution

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

6 Documentation

- Bulletins de sécurité de CISCO :
<http://cisco.com/warp/public/707/cisco-sa-20060920-docsis.shtml>

Gestion détaillée du document

21 septembre 2006 version initiale.