



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 février 2005
N° CERTA-2005-AVI-047

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des équipements IP/VC de Cisco

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-047>

Gestion du document

Référence	CERTA-2005-AVI-047
Titre	Vulnérabilité des équipements IP/VC de Cisco
Date de la première version	03 février 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Cisco
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

Prise de contrôle à distance de l'équipement.

2 Systèmes affectés

- Cisco IPVC-3510-MCU ;
- Cisco IPVC-3520-GW-2B ;
- Cisco IPVC-3520-GW-4B ;
- Cisco IPVC-3520-GW-2V ;
- Cisco IPVC-3520-GW-4V ;
- Cisco IPVC-3520-GW-2B2V ;
- Cisco IPVC-3525-GW-1P ;
- Cisco IPVC-3530-VTA.

3 Description

Selon Cisco, des noms de communauté SNMP non modifiables sont présents dans les équipements de visio-conférence cités ci-dessus.

Via le biais de requêtes SNMP, il est alors possible pour un utilisateur distant mal intentionné de créer de nouvelles sessions ou même re-router des sessions existantes sur les équipements vulnérables.

4 Contournement provisoire

Filter le trafic SNMP (port 161/UDP et 162/UDP) vers ces équipements.

5 Solution

Se référer au bulletin de sécurité du constructeur pour l'obtention des correctifs.

6 Documentation

Bulletin de sécurité Cisco "Default SNMP community strings in Cisco IP/VC products" du 2 février 2005 :
<http://www.cisco.com/warp/public/707/cisco-sa-20050202-ipvc.shtml>

Gestion détaillée du document

03 février 2005 version initiale.