Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 mars 2007
N° CERTA-2007-AVI-104

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans les Cisco Catalyst

Gestion du document

Référence	CERTA-2007-AVI-104
Titre	Vulnérabilités dans les Cisco Catalyst
Date de la première version	01 mars 2007
Date de la dernière version	–
Source(s)	Bulletins de sécurité CISCO du 28 février 2007
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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

- les séries Cisco Catalyst 6000 ;
- les séries Cisco Catalyst 6500 ;
- les séries Cisco 7600.

3 Résumé

Deux vulnérabilités ont été identifiées dans certains produits Cisco Catalyst. Elles permettraient à une personne malveillante distante de prendre le contrôle du système vulnérable, ou du moins le perturber.

4 Description

Deux vulnérabilités ont été identifiées dans certains produits Cisco Catalyst.

1. La première vulnérabilité concerne le module NAM (pour *Network Analysis Module*). Ce dernier sert à la surveillance et l'analyse de trafic du réseau, par le biais de RMON (*Remote Monitoring*), RMON2 et d'autres MIBs (*Management Information Bases*). Ces informations sont accessibles à distance par le protocole *Simple Network Management Protocol* ou SNMP. Cependant, les échanges SNMP entre les modules NAMs et le système Catalyst ne seraient pas correctement sécurisés, notamment au niveau de l'authentification. Cela pourrait permettre à un utilisateur malveillant distant de prendre le contrôle, via SNMP, du système vulnérable.
2. la seconde vulnérabilité concernerait la manipulation par des interfaces de routage nommées Route Processor (ou MSFC) de paquets MPLS. Ce protocole, *Multiprotocol Label Switching*, sert à fournir un service unifié de transport de données, en permettant la commutation des paquets marqués, ou labélisés. La vulnérabilité ne nécessite cependant pas que le protocole soit configuré pour fonctionner. Une personne malveillante pourrait envoyer des paquets MPLS spécialement construits pour perturber le système vulnérable.

5 Solution

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

6 Documentation

- Bulletin de sécurité Cisco ID 81865 du 28 février 2007 :
  http://www.cisco.com/warp/public/707/cisco-sa-20070228-mpls.shtml
- Bulletin de sécurité Cisco ID 81863 du 28 février 2007 :
  http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml

Gestion détaillée du document

01 mars 2007 version initiale.