Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 mars 2001
N° CERTA-2001-AVI-026

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans les commutateurs CISCO IOS

Gestion du document

Référence	CERTA-2001-AVI-026
Titre	Vulnérabilités dans les commutateurs CISCO IOS
Date de la première version	05 mars 2001
Date de la dernière version	–
Source(s)	Avis 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

- Accès aux informations du système ;
- contournement des règles de sécurité ;
- risques d'usurpation d'adresses IP.

2 Systèmes affectés

Commutateurs CISCO IOS.

3 Résumé

De nombreuses vulnérabilités ont été découvertes dans les commutateurs CISCO IOS.
Cinq vulnérabilités concernent les communautés SNMP (Simple Network Management Protocol) et une autre vulnérabilité concerne le protocole TCP.

4 Description

4.1 Vulnérabilités dans les communautés SNMP

4.1.1 Première vulnérabilité

Le standard ILMI (Interim Local Management Interface) permet de gérer les interfaces ATM des équipements d'interconnexion. Un utilisateur mal intentionné peut, en utilisant le nom de communauté ILMI, avoir accès à la MIB (Management Information Base) en lecture, voire en écriture pour certaines données. Un grand nombre de requêtes lecture-écriture peut également entraîner un déni de service.

Cette vulnérabilité affecte les systèmes IOS 11.x et 12.0.

4.1.2 Deuxième vulnérabilité

Un utilisateur mal intentionné peut, par le biais d'une vulnérabilité dans le séquencement des commandes pour la configuration du service SNMP, créer un nom de communauté non désiré afin d'accéder en lecture à certaines données.

Cette vulnérabilité affecte les systèmes IOS 12.x.

4.1.3 Troisième vulnérabilité

Une vulnérabilité de la fonction «informs» concernant le partage d'informations permet, par le biais de la communauté créée pour l'échange d'informations, d'interroger la MIB locale.

Cette vulnérabilité affecte les systèmes IOS 12.x.

4.1.4 Quatrième vulnérabilité

Un utilisateur mal intentionné peut, en listant la MIB View-Based Access Control, obtenir le nom d'une communauté ayant les droits lecture-écriture.

Cette vulnérabilité affecte les systèmes IOS 12.x.

4.1.5 Cinquième vulnérabilité

Une vulnérabilité à été découverte dans un nom de communauté ayant les droits lecture-écriture assurant l'administration de modem «câble».

Cette vulnérabilité affecte les systèmes IOS 12.x.

4.2 Vulnérabilité du protocole TCP

Un utilisateur distant mal intentionné peut, par le biais d'une vulnérabilité de l'ISN (Gestion du numéro de séquence initial), prévoir les valeurs qui vont être utilisées par le système et effectuer des usurpations d'adresses IP (spoofing)

5 Solution

Les différents correctifs, en fonction des versions d'IOS, sont disponibles sur le site CISCO :
http://www.cisco.com

6 Documentation

Vulnérabilités concernant les communautés SNMP :
http://www.cisco.com/warp/public/707/ios-snmp-ilmi-vuln-pub.shtml
http://www.cisco.com/warp/public/707/ios-snmp-community-vulns-pub.shtml

Vulnérabilité concernant le protocole TCP :
http://www.cisco.com/warp/public/707/ios-tcp-isn-random-pub.shtml

Gestion détaillée du document

05 mars 2001 version initiale.