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 avril 2004
N° CERTA-2004-AVI-138

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sur Cisco IOS

Gestion du document

Référence	CERTA-2004-AVI-138
Titre	Vulnérabilité sur Cisco IOS
Date de la première version	21 avril 2004
Date de la dernière version	–
Source(s)	Avis de sécurité Cisco 20040420
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

Déni de service.

2 Systèmes affectés

Routeurs et commutateurs Cisco qui utilisent une verion IOS vulnérable :

- 12.0(23)S4;
- 12.0(23)S5;
- 12.0(24)S4;
- 12.0(24)S5;
- 12.0(26)S1;
- 12.0(27)S;
- 12.0(27)SV;
- 12.0(27)SV1;
- 12.1(20)E;
- 12.1(20)E1;
- 12.1(20)E2;
- 12.1(20)EA1;

- 12.1(20)EW;
- 12.1(20)EW1;
- 12.1(20)EC;
- 12.1(20)EC1;
- 12.2(12g);
- 12.2(12h);
- 12.2(20)S;
- 12.2(20)S1;
- 12.2(21);
- 12.2(21a);
- 12.2(23);
- 12.3(2)XC1;
- 12.3(2)XC2;
- 12.3(5);
- 12.3(5a);
- 12.3(5b);
- 12.3(6);
- 12.3(4)T;
- 12.3(4)T1;
- 12.3(4)T2;
- 12.3(4)T3;
- 12.3(5a)B;
- 12.3(4)XD;
- 12.3(4)XD1.

3 Résumé

Une vulnérabilité présente dans le traitement des en-têtes des messages SNMP sur Cisco IOS, provoque un rédémarrage du systéme vulnérable.

4 Description

Le protocole SNMP (Simple Network Management Protocol) est le protocole utilisé pour visualier et contrôler un équipement du réseau à distance.

Une vulnérabilité dans le traitement des en-têtes de messages SNMP sur Cisco IOS permet à un utilisateur mal intentionné, via l'envoi de paquets SNMP malicieusement construits, de réaliser un déni de service sur le système vulnérable.

5 Solution

Appliquer le correctif correspondant à votre version de Cisco IOS (cf. avis de sécurité CISCO, section documentation).

6 Documentation

- Avis de sécurité Cisco :
  http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml
- Avis de sécurité de US-CERT TA04-111B :
  http://www.us-cert.gov/cas/techalerts/TA04-111B.html

Gestion détaillée du document

21 avril 2004 version initiale.