

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : vulnérabilité de SNMP sur 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-2002-AVI-032>

Gestion du document

Référence	CERTA-2002-AVI-032
Titre	vulnérabilité de SNMP sur CISCO
Date de la première version	13 février 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité 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

Déni de service.

2 Systèmes affectés

La plupart des appareils CISCO. Pour savoir si votre système est affecté, se référer au bulletin de sécurité CISCO (paragraphe Documentation).

3 Résumé

Un utilisateur mal intentionné peut utiliser une vulnérabilité de l'agent SNMP pour causer un redémarrage à distance des équipements CISCO.

4 Description

Les tests effectués par l'université finlandaise d'Oulu ont mis en évidence la présence de vulnérabilités dans les routines de décodage et de traitement des messages SNMP dans de nombreuses implémentations (se référer au bulletin d'alerte CERTA-2002-ALE-004 du CERTA).

Une vulnérabilité de l'agent SNMP, permet à un utilisateur mal intentionné de faire redémarrer un appareil CISCO. Cette vulnérabilité, de type débordement de mémoire, est exploitable à distance.

5 Contournement provisoire

- Couper le service SNMP à l'aide de la commande de configuration :
`no snmp-server;`
- utiliser les capacités de filtrage (Access Control List) de chaque équipement CISCO afin de restreindre l'accès aux ports 161/UDP et 162/UDP uniquement à la station d'administration du réseau au moyen des commandes de configuration suivantes :
`access-list 100 permit ip host x.x.x.x any`
`access-list 100 deny udp any any eq snmp`
`access-list 100 deny udp any any eq snmptrap`
`access-list 100 permit ip any any`
Où x.x.x.x est l'adresse IP de la station d'administration du réseau.
- Filtrer les ports 161/udp et 162/UDP et 1993/TCP utilisés par le protocole SNMP V1 au niveau du garde-barrière afin d'empêcher l'exploitation de ces vulnérabilités depuis l'Internet visant les appareils présents à l'intérieur du réseau.

6 Solution

Se référer au bulletin de sécurité CISCO (voir paragraphe Documentation) pour appliquer le correctif selon l'appareil utilisé.

7 Documentation

Bulletin de sécurité CISCO :
<http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml>

Gestion détaillée du document

13 février 2002 version initiale.