

Affaire suivie par :  
CERTA

## BULLETIN D'ALERTE DU CERTA

### Objet : Multiples implémentations de SNMP V1 vulnérables

---

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-ALE-004>

---

### Gestion du document

Référence	CERTA-2002-ALE-004
Titre	Multiples implémentations de SNMP V1 vulnérables
Date de la première version	13 février 2002
Date de la dernière version	-
Source(s)	Avis CA-2002-03 du CERT/CC
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 ;
- exécution de code arbitraire à distance.

## 2 Systèmes affectés

A la date de parution de ce document, des tests sont encore en cours.

Consulter régulièrement l'avis du CERT/CC (cf. section documentation) pour obtenir la liste des systèmes affectés.

## 3 Résumé

SNMP (Single Network Management protocole) est un protocole utilisé dans le domaine de la supervision de réseaux. Il permet à deux entités, un agent et une console, d'échanger des messages.

L'agent SNMP est disponible sur de nombreux équipements : dans les systèmes d'exploitation (sous forme de service) mais aussi dans les équipements réseaux (routeurs, commutateurs...), les imprimantes, etc.

Un groupe de recherche de l'université de OULU en Finlande, a mis au point une série de tests démontrant la vulnérabilité de nombreuses implémentations du protocole SNMP V1.

## 4 Description

SNMP est un protocole permettant à deux entités d'échanger des messages. Ce protocole est décrit dans le document rfc 1157 (SNMP V1) : un agent répond au sollicitation d'une console (requêtes GET, GET\_NEXT ou SET) et peut également envoyer des messages de façon asynchrone (TRAP).

Les tests effectués à l'université de OULU mettent en évidence que de nombreuses vulnérabilités ( débordement de mémoire, chaîne de format, ...) existent dans les routines de décodage et de traitement des messages SNMP.

L'exploitation de ces vulnérabilités peut conduire à un déni de service et même l'exécution de code arbitraire à distance sur les plate-formes considérées.

## 5 Contournement provisoire

- Ne démarrer le service SNMP que si celui-ci est nécessaire ;
- utiliser les capacités de filtrage que possèdent certains agent SNMP. Par exemple, il est possible d'indiquer à l'agent qu'il ne peut répondre qu'aux requêtes des consoles SNMP dont l'adresse IP est présente dans un fichier de configuration ;
- ne pas utiliser les noms de communautés positionnés lors de l'installation par défaut ;
- filtrer les ports 161/udp et 162/udp utilisés par le protocole SNMP V1 au niveau du garde-barrière afin d'empêcher l'exploitation de ces vulnérabilités depuis l'Internet.

A noter que des services RPC ( 100122 snmp, 100138 snmpV2, 100249 snmpXdmid) et certains ports d'utilisation moins courante sont également concernés :

Port	Description
161/tcp et 162/tcp	SNMP sur tcp
199/tcp et 199/udp	smux
391/tcp et 391/udp	SynOptics relay port
705/tcp	agentX
1993/tcp et 1993/udp	Cisco SNMP port

## 6 Solution

Se référer à l'avis du CERT/CC (cf. section documentation) pour obtenir la liste des systèmes affectés et les correctifs disponibles.

## 7 Documentation

- Avis de sécurité CA-2002-03 "Multiple vulnerabilities in many implementations of the Simple Network Management Protocol (SNMP)" du Cert/CC :  
<http://www.cert.org/advisories/CA-2002-03.html>
- Rfc 1157 "A Simple Network Management Protocol (SNMP)" :  
<http://www.ietf.org/rfc/rfc1157.txt>
- PROTOS Test-Suite c06-snmpv1 :  
<http://www.ee.oulu.fi/research/ouspg/protos/testing/c06/snmpv1/index.html>

## Gestion détaillée du document

13 février 2002 version initiale.