Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 février 2002
N° CERTA-2002-AVI-031

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de l'agent SNMP sous Solaris

Gestion du document

Référence	CERTA-2002-AVI-031
Titre	Vulnérabilité de l'agent SNMP sous Solaris
Date de la première version	13 février 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité #00215 de Sun
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

Elévation de privilèges.

2 Systèmes affectés

Solaris versions 6, 7 et 8 (plate-forme sparc et x86) utilisant Sun Solstice Enterprise Agent.

3 Résumé

Un utilisateur mal intentionné peut utiliser une vulnérabilité de l'agent SNMP (Sun Solstice Entreprise Master Agent) sous Solaris pour exécuter du code arbitraire à distance avec les privilèges de l'administrateur `root`.

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, `snmpdx`, permet à un utilisateur mal intentionné d'exécuter du code arbitraire avec les privilèges de l'administrateur `root`. Cette vulnérabilité, de type débordement de mémoire, est exploitable à distance.

5 Contournement provisoire

- Ne démarrer le service SNMP via le script `/etc/rc3.d/S76snmpdx` que si celui-ci est nécessaire ;
- utiliser les capacités de filtrage (Access Control List) de l'agent SNMP ;
- 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.

6 Solution

Se référer au bulletin de sécurité de SUN (cf. section Documentation) pour la disponibilité des correctifs.

7 Documentation

- Bulletin de Sécurité #00215 "snmpdx" disponible à l'adresse suivante :
  http://sunsolve.sun.com/pub-cgi/secBulletin.pl/
- Documentation "Solstice Enterprise Agents" :
  http://www.sun.com/software/entagents/docs.html

Gestion détaillée du document

13 février 2002 version initiale.