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 juin 2002
N° CERTA-2002-AVI-117

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des agents SNMP sous Solaris

Gestion du document

Référence	CERTA-2002-AVI-117
Titre	Vulnérabilité des agents SNMP sous Solaris
Date de la première version	05 juin 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité #219 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 maître SNMP (`snmpdx`) et du sous-agent SNMP (`mibiisa`) sous Solaris pour exécuter du code arbitraire à distance avec les privilèges de l'administrateur `root`.

4 Description

`snmpdx` est un agent SNMP maître transférant les requêtes SNMP reçues sur le port 161/UDP vers des sous-agents SNMP (dont `mibiisa`).

Deux vulnérabilités ont été découvertes dans ces agents :

– `snmpdx` présente une vulnérabilité de type chaîne de format ;

– `mibiisa` présente une vulnérabilité de type débordement de mémoire.

Ces vulnérabilités permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance avec les privilèges de l'administrateur `root`.

5 Contournement provisoire

Ne démarrer le service SNMP que si celui-ci est nécessaire.
Par défaut, ce dernier est démarré via le script `/etc/rc3.d/S76snmpdx`.

6 Solution

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

7 Documentation

– Bulletin de Sécurité #00219 "SEA SNMP" 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

– Bulletin de sécurité "SEA SNMP -Buffer overflow and Format String Vulnerabilities in Solaris" d'Entercept :
http://www.entercept.com/news/uspr/06-03-02.asp

Gestion détaillée du document

05 juin 2002 version initiale.