Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 mars 2001
N° CERTA-2001-ALE-004

**Affaire suivie par :**
CERTA

# BULLETIN D'ALERTE DU CERTA

## Objet : Vulnérabilité dans le démon snmpXdmid sous Sun Solaris



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2001-ALE-004 |
| Titre | Vulnérabilité dans le démon snmpXdmid sous Sun Solaris |
| Date de la première version | 30 mars 2001 |
| Date de la dernière version | – |
| Source(s) | Bugtraq |
| 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

Compromission des machines Sun Solaris.

## 2 Systèmes affectés

Sun Solaris 2.6, 2.7 et 2.8 avec le daemon snmpXdmid.

## 3 Résumé

Une faille dans le démon snmpXdmid a été récemment découverte. Celle-ci permet à une personne mal intentionnée de prendre le contrôle de la machine. Cette faille est actuellement massivement exploitée par les pirates.

## 4 Description

Le démon snmpXdmid est un service RPC effectuant la traduction des standards d'administration à distance SNMP (Simple Network Management Protocol) et DMI (Desktop Management Protocol). Il est installé par défaut sur Sun Solaris. La version sur Sun Solaris contient une vulnérabilité qui permet à une personne mal intentionnée de prendre le contrôle d'une machine.

Lorsqu'une machine est compromise par cette faille, des fichiers sont installés par le pirate.
Parmi ceux-ci se trouvent :

- Un "rootkit" pour Sun Solaris (reprogrammation de du, find, ls, netstat, passwd, ping, psr, su) ;
- Un renifleur de mots de passe ;
- Un nettoyeur de fichiers journaux ;
- Des outils pour installer des portes dérobées (l'une d'entre elles se dissimule sous le démon identd).

# 5 Contournement provisoire

- Filtrer les ports :
  - 111/tcp (sunrpc - portmapper) ;
  - 6500/udp ;
  - 113/tcp (identd).
- Arrêter le service smpdXdmid en renommant le fichier /etc/rc?.d/S??dmi en /etc/rc?.d/K07dmi (où ? correspond au niveau de lancement) et en lançant la commande '/etc/init.d/init.dmi stop'. Il est également recommandé de changer les droits d'accès du binaire en utilisant la commande : 'chmod 000 /usr/lib/dmi/snmpXdmid'.

# 6 Solution

Appliquer le patch correctif de Sun sur snmpXdmid lorsque celui-ci sera rendu publique.

# 7 Documentation

Bugtraq

# Gestion détaillée du document

**30 mars 2001** version initiale.