Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 juin 2002
N° CERTA-2001-AVI-088-001

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

**Objet : Vulnérabilité de SnmpXdmid sur Sun**

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-2001-AVI-088

## Gestion du document

| | |
|---|---|
| Référence | CERTA-2001-AVI-088-001 |
| Titre | Vulnérabilité de SnmpXdmid sur Sun |
| Date de la première version | 31 août 2001 |
| Date de la dernière version | 28 juin 2002 |
| Source(s) | Avis CA-2001-05 CERT/CC<br>Alerte CERTA-2001-ALE-004 et ALE-007<br>Bulletin de sécurité #00207 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

Exécution de code arbitraire à distance avec les privilèges de `root`.

## 2 Systèmes affectés

Les versions de SunOS 5.8, 5.8x86, 5.7, 5.7_x86, 5.6 et 5.6_x86 sont vulnérables.

## 3 Résumé

Une vulnérabilité de SnmpXdmid sous Sun Solaris permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance avec les privilèges de `root`.

Cette faille a déja été décrite dans l'alerte CERTA-2001-ALE-004.

# 4 Description

Le *daemon* `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.

Une vulnérabilité de `SnmpXdmid` sous Sun Solaris permet à un utilisateur mal intentionné de prendre le contrôle d'une machine à distance.

# 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 correctif de Sun, selon la version, disponible sur
http://sunsolve.sun.com/securitypatches :

- Pour SunOS 5.8 : 108869-07 ;
- pour SunOS 5.8_x86 : 108870-07 ;
- pour SunOS 5.7 : 107709-15 ;
- pour SunOS 5.7_x86 : 107710-15 ;
- pour SunOS 5.6 : 106787-15 ;
- pour SunOS 5.6_86 : 106872-15 ;

# 7 Documentation

- Alerte CERTA-2001-ALE-004 : Vulnérabilité dans le démon snmpXdmid sous Sun Solaris :
- Bulletin de sécurité #00207 de Sun :
  http://sunsolve.sun.com/pub-cgi/secBulletin.pl
- Avis CA-2001-05 du CERT/CC :
  http://www.cert.org/advisories/CA-2001-05.html

# Gestion détaillée du document

**31 août 2001** version initiale.

**28 juin 2002** première révision : référence erronée du bulletin de sécurité du CERT/CC