Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 janvier 2001
N° CERTA-2001-AVI-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans ARP sous SunOS

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-004

Gestion du document

Référence	CERTA-2001-AVI-004
Titre	Vulnérabilité dans ARP sous SunOS
Date de la première version	15 janvier 2001
Date de la dernière version	–
Source(s)	Avis de sécurité de Sun Microsystems
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 ;
- exécution de code arbitraire avec privilèges ;
- accès `root` en local.

2 Systèmes affectés

Toutes versions de SunOS ou Solaris inférieures à Solaris 8.

3 Résumé

La commande `ARP` est un outil permettant de manipuler les tables d'adressage des cartes *ethernet*. Une vulnérabilité de cet utilitaire permet à un utilisateur mal intentionné d'exécuter du code ou d'obtenir un *shell* `root`.

4 Description

La commande `arp` appartient au groupe `bin` et possède le bit `SetGID`. De plus cet outil possède une vulnérabilité permettant d'effectuer un débordement de mémoire.

Un utilisateur mal intentionné peut utiliser cette vulnérabilité dans le but d'obtenir un accès à un *shell*, ou bien d'exécuter du code avec les privilèges de `bin` ou même de `root`.

5 Solution

Appliquer le correctif de sun Microsystems selon la version du système, à l'adresse :
http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access .

- SunOS 5.7 : 109709-01
- SunOS 5.7_x86 : 109710-01
- SunOS 5.6 : 109719-01
- SunOS 5.6_x86 : 109720-01
- SunOS 5.5.1 : 109721-01
- SunOS 5.5.1_x86 : 109722-01
- SunOS 5.5 : 109707-01
- SunOS 5.5_x86 : 109708-01
- SunOS 5.4 : 109723-01
- SunOS 5.4_x86 : 109724-01

6 Documentation

Bulletin de sécurité #00200 de Sun Microsystems :
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/200&type=0&nav=sec.sba

Gestion détaillée du document

15 janvier 2001 version initiale.