Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 septembre 2002
N° CERTA-2002-AVI-210

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de `aspppls` sous solaris 8

Gestion du document

Référence	CERTA-2002-AVI-210
Titre	Vulnérabilité de `aspppls` sous solaris 8
Date de la première version	17 septembre 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité #46903 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 en local ;
- corruption de fichiers ;
- déni de service.

2 Systèmes affectés

Cette vulnérabilité n'affecte que la version 8 de Solaris.

3 Résumé

Une vulnérabilité de `aspppls` sous solaris 8 permet à un utilisateur local d'accéder aux privilèges de l'administrateur `root`.

4 Description

`aspppls` (*ASynchronous PPP Login Service* est un service d'authentification d'`aspppd`. Il est démarré lorsqu'un utilisateur ayant un compte `ppp` se connecte au serveur `aspppd`.

Une mauvaise gestion des fichiers temporaires dans `aspppls` permet à un utilisateur connecté localement de corrompre des fichiers du système et d'obtenir les privilèges de l'administrateur `root`.

5 Contournement provisoire

- Supprimer `aspppls` s'il n'est pas utilisé.
- En attendant de pouvoir appliquer le correctif de Sun, supprimer le bit `SUID` de l'exécutable `aspppls` au moyen de la commande suivante :
  ```
  chmod u-s /usr/sbin/aspppls
  ```

6 Solution

Consulter le bulletin de sécurité #46903 de Sun (voir le paragraphe Documentation) pour connaître la disponibilité des correctifs.

7 Documentation

Bulletin de sécurité #46903 de Sun :
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F46903

Gestion détaillée du document

17 septembre 2002 version initiale.