Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 septembre 2001
N° CERTA-2001-AVI-090

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de in.lpd sous Solaris

Gestion du document

Référence	CERTA-2001-AVI-090
Titre	Vulnérabilité de in.lpd sous Solaris
Date de la première version	03 septembre 2001
Date de la dernière version	–
Source(s)	Avis du CERT/CC CA-2001-015 Bulletin de sécurité Sun #00206
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.

2 Systèmes affectés

SonOS 5.8, 5.8_x86, 5.7, 5.7_x86, 5.6, 5.6_x86.

3 Résumé

Une vulnérabilité du *daemon* `in.lpd` sous SunOS permet à un utilisateur mal intentionné d'exécuter du code arbitraire avec les privilèges du compte associé à ce *daemon* (par défaut `root`.

4 Description

`in.lpd` est le service d'impression `BSD` sous Solaris.

Une vulnérabilité de ce *daemon* permet à un utilisateur local ou distant d'effectuer un débordement de mémoire pouvant conduire à un arrêt du service ou bien à l'exécution de code arbitraire sur le serveur victime avec les privilèges de ce *daemon*.

Par défaut les privilèges du *daemon* `in.lpd`, sont ceux de `root`.

5 Contournement provisoire

Désactiver ou supprimer `in.lpd` s'il n'est pas utilisé sur cette machine.

6 Solution

Télécharger le correctif de Sun selon les versions à l'adresse suivante :
http://sunsolve.sun.com/securitypatch

- Pour SunOS 5.8 : 109320-04
- Pour SunOS 5.8_x86 : 109321-04
- Pour SunOS 5.7 : 107115-09
- Pour SunOS 5.7_x86 : 107116-09
- Pour SunOS 5.6 : 106235-09
- Pour SunOS 5.6_x86 : 106236-09

7 Documentation

- Bulletin de sécurité Sun numéro #00206 à paraître sur :
  http://sunsolve.sun.com/pub-cgi/secBulletin.pl
- Avis de sécurité du CERT/CC :
  http://www.cert.org/advisories/CA-2001-15.html

Gestion détaillée du document

03 septembre 2001 version initiale.