Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 avril 2003
N° CERTA-2003-AVI-070

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de la commande lpq sous Solaris

Gestion du document

Référence	CERTA-2003-AVI-070
Titre	Vulnérabilité de la commande lpq sous Solaris
Date de la première version	02 avril 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité #52443 de Sun Bulletin de sécurité SA2003-02 de nsfocus
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.

2 Systèmes affectés

Solaris version 2.5.1 à 7 incluse. Solaris 8 et Solaris 9 ne sont pas affectées.

3 Résumé

Une vulnérabilité présente dans la commande `lpq` permet à un utilisateur mal intentionné de réaliser une élévation de privilèges.

4 Description

La commande `lpq` est utilisée pour visualiser le contenu des files d'impression. Une vulnérabilité de type débordement de mémoire présente dans cette commande peut être exploitée par un utilisateur mal intentionné pour obtenir les privilèges du super-utilisateur `root`.

5 Contournement provisoire

En attendant d'appliquer les correctifs, enlever le drapeau `suid` sur l'exécutable `/usr/bin/lpstat` (la commande `lpq` est en réalité un lien sur cet exécutable).

6 Solution

Appliquez les correctifs fournis par l'éditeur. Bulletin de sécurité #52443 de Sun :
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F52443

7 Documentation

- Référence CVE CAN-2003-0091 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0091
- Bulletin de sécurité SA2003-02 "Solaris lpq stack buffer overflow vulnerability" de nsfocus :
  http://www.nsfocus.com/english/homepage/research/0302.htm

Gestion détaillée du document

02 avril 2003 version initiale.