Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 décembre 2000
N° CERTA-2000-AVI-087

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Problèmes de validation pour LPRng

Gestion du document

Référence	CERTA-2000-AVI-087
Titre	Problèmes de validation pour LPRng
Date de la première version	13 décembre 2000
Date de la dernière version	–
Source(s)	Avis CA-2000-22 du CERT/CC
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

- Déni de service ;
- Exécution de code arbitraire.

2 Systèmes affectés

La plupart des systèmes proposant le module LPRng.

3 Résumé

LPRng est un module d'impression équivalent à `lpd` de plus en plus présent dans la plupart des distributions Unix ou Linux.

Une vulnérabilité de ce module permet à un utilisateur mal intentionné d'effectuer à distance un débordement de mémoire pouvant conduire à l'exécution de code arbitraire sur la machine victime.

4 Description

Une vulnérabilité liée à l'exploitation de la librairie `glibc` (Cf. Alerte CERTA-2000-ALE-014 : Vulnérabilité dans la bibliothèque glibc sous Unix) permet à un utilisateur mal intentionné d'effectuer un débordement de mémoire à distance dans le module LPRng. Ce débordement de mémoire peut avoir comme conséquence un déni de service d'impression local ou en réseau, mais peut aussi, s'il est bien mené, conduire à l'exécution de code arbitraire.

5 Contournement provisoire

Le port utilisé par le module d'impression LPRng est le port 515 en TCP. Son accès de l'extérieur du réseau doit être bloqué par le garde-barrière.

6 Solution

Supprimer LPRng de toute machine ne l'utilisant pas.
Consulter l'éditeur du système pour obtenir le correctif à appliquer.
Pour les systèmes :

- RedHat, appliquer le correctif suivant :
  http://www.redhat.com/support/errata/RHSA-2000-065-06.html
- Pour Caldera :
  http://www.calderasystems.com/support/security/advisories/CSSA-2000-033.0.txt
- Pour les anciennes versions de FreeBSD :
  ftp://FreeBSD.org/pub/FreeBSD/CERT/advisorie/FreeBSD-SA-00:56.lprng.asc

`Nota` **:** Si l'éditeur n'a pas de correctif, ou si LPRng est un ajout externe à la distribution utilisée, passer à la version 3.6.25 :
ftp://ftp.astart.com/pub/LPRng/LPRng/LPRng-3.6.25.tgz

7 Documentation

L'avis de sécurité du CERT/CC :
http://www.cert.org/advisories/CA-2000-22.html
http://www.kb.cert.org/vuls/id/382365
`Nota` **:** Suse n'est pas vulnérable de par l'ancienneté de leur module LPRng, mais a tout de même diffusé un bulletin pour confirmer l'information :
http://lists.suse.com/archives/suse-security/2000-Sep/0259.html

Gestion détaillée du document

13 décembre 2000 version initiale.