Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 novembre 2001
N° CERTA-2001-AVI-148

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le service d'impression sous HP-UX

Gestion du document

Référence	CERTA-2001-AVI-148
Titre	Vulnérabilité dans le service d'impression sous HP-UX
Date de la première version	22 novembre 2001
Date de la dernière version	–
Source(s)	Avis CA-2001-32 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

Serveurs HP9000 utilisant les versions suivantes:
- HP-UX version 10.01;
- HP-UX version 10.10;
- HP-UX version 10.20;
- HP-UX version 11.00;
- HP-UX version 11.11.

3 Résumé

Une vulnérabilité présente dans le service d'impression `rlpdaemon` de HP-UX permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance avec les privilèges de `root`.

4 Description

Le service d'impression `rlpdaemon` sous HP-UX permet le partage des imprimantes sur un réseau.

L'exploitation d'une vulnérabilité de type débordement de mémoire présente dans ce service permet à un utilisateur mal intentionné d'exécuter du code arbitraire avec les privilèges de `root`.

Cette vulnérabilité est exploitable à distance.

5 Contournement provisoire

Arrêter le service `rlpdaemon` en attendant l'application des correctifs.

A défaut, filtrer les accès au port 515/tcp utilisé par ce service afin de limiter l'accès aux seuls clients autorisés.

6 Solution

Un correctif sera publié par Hewlett-Packard avec les références suivantes:

- HPCO_25107 pour HP-UX version 10.01;
- HPCO_25108 pour HP-UX version 10.10;
- HPCO_25109 pour HP-UX version 10.20;
- HPCO_25110 pour HP-UX version 11.00;
- HPCO_25111 pour HP-UX version 11.11.

7 Documentation

- Bulletin de sécurité #0176 de Hewlett-Packard disponible sur le site http://itrc.hp.com ;
- Avis CA-2001-32 du CERT/CC: http://www.cert.org/advisories/CA-2001-32.html

Gestion détaillée du document

22 novembre 2001 version initiale.