

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de rlpdaemon sous HP-UX

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2001-AVI-091>

Gestion du document

Référence	CERTA-2001-AVI-091
Titre	Vulnérabilité de rlpdaemon sous HP-UX
Date de la première version	05 septembre 2001
Date de la dernière version	–
Source(s)	Bulletin de sécurité HP HPSBUX0108-163
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

HP-UX 10.01, 10.10, 10.20, 11.11, 11.20.

3 Résumé

Une vulnérabilité du daemon `rlpdaemon` sous HP-UX permet à un utilisateur mal intentionné d'exécuter du code arbitraire avec les privilèges du compte associé à ce daemon.

4 Description

`rlpdaemon` est un service d'impression sous HP-UX adapté des sources BSD.

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 `rlpdaemon` est installé et actif lors de l'installation du système.

5 Contournement provisoire

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

6 Solution

Appliquer le correctif selon la version sur le site suivant :

<http://itrc.hp.com> .

- Pour HP-UX 10.01 : PHCO_24697
- Pour HP-UX 10.10 : PHCO_24698
- Pour HP-UX 10.20 : PHCO_24699
- Pour HP-UX 11.00 : PHCO_24700
- Pour HP-UX 11.11 : PHCO_24701

7 Documentation

- Avis de sécurité HPSBUX0108-163 :
<http://itrc.hp.com>
- Bulletin de sécurité du CIAC :
<http://www.ciac.org/ciac/l-134.shtml>

Gestion détaillée du document

05 septembre 2001 version initiale.