



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 juillet 2004
N° CERTA-2004-AVI-219

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de rlpr

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-2004-AVI-219>

Gestion du document

Référence	CERTA-2004-AVI-219
Titre	Multiples vulnérabilités de rlpr
Date de la première version	02 juillet 2004
Date de la dernière version	–
Source(s)	Bulletin d'alerte Debian DSA-524-1
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

rp1rd en version 2.0.4.
Les versions antérieures pourraient être affectées.

3 Résumé

Une vulnérabilité dans la fonction de journalisation du démon rlprd permet l'exécution de code arbitraire à distance. Une deuxième vulnérabilité permet l'élévation de privilèges.

4 Description

Le paquetage rlpr contient des remplacements compatibles BSD pour les programmes lpr, lpq et lprm. Il permet aussi d'imprimer sur une imprimante locale des fichiers se trouvant sur une machine distante.

La fonctionnalité de journalisation du paquetage `rlpr` appelle `syslog` sans spécifier le format. Un utilisateur mal intentionné peut, en provoquant une erreur au moment de la connexion sur le serveur `rlprd` distant, exécuter du code arbitraire sur le serveur (CAN-2004-0393).

Une vulnérabilité de type dépassement de tampon affecte la fonction `msg()` dans `rlpr`. L'exploitation de cette vulnérabilité permet une élévation de privilèges (CAN-2004-0454).

5 Solution

Se référer au bulletin de l'éditeur pour la disponibilité des correctifs (voir Documentation).

6 Documentation

- Bulletin de sécurité Debian DSA-524-1 du 19 juin 2004 :
<http://www.debian.org/security/2004/dsa-524>
- Référence CVE CAN-2004-0393 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0393>
- Référence CVE CAN-2004-0454 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0454>

Gestion détaillée du document

02 juillet 2004 version initiale.