



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 octobre 2003
N° CERTA-2003-AVI-154-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans lsh

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-2003-AVI-154>

Gestion du document

Référence	CERTA-2003-AVI-154-001
Titre	Vulnérabilité dans lsh
Date de la première version	22 septembre 2003
Date de la dernière version	02 octobre 2003
Source(s)	
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

- Pour la branche stable, lsh versions 1.4.2 et antérieures ;
- Pour la branche de développement, lsh versions 1.5, 1.5.1, 1.5.2.

3 Résumé

Une vulnérabilité dans lsh permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance avec les droits de root.

4 Description

lsh est une implémentation GNU du protocole SSH (Secure SHell). Une vulnérabilité de type débordement de mémoire, permet à un utilisateur mal intentionné d'exécuter du code avec les droits de root.

5 Solution

Mettre à jour lsh en version 1.4.3 (branche stable) ou 1.5.3 (branche de développement). Téléchargement de lsh :

<http://www.lysator.liu.se/~nisse/archive/>

6 Documentation

- Site de lsh :
<http://www.lysator.liu.se/~nisse/lsh/>
- Avis de sécurité SuSE Linux SuSE-SA:2003:041 :
http://www.suse.de/de/security/2003_041_lsh.html

Gestion détaillée du document

22 septembre 2003 version initiale.

02 octobre 2003 ajout du bulletin de sécurité SuSE Linux.