Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 septembre 2004
N° CERTA-2004-AVI-294-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de lha

Gestion du document

Référence	CERTA-2004-AVI-294-002
Titre	Vulnérabilité de lha
Date de la première version	02 septembre 2004
Date de la dernière version	28 septembre 2004
Source(s)	Bulletin de sécurité RedHat RHSA-2004:323 du 01 septembre 2004
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

lha version 1.14 et versions antérieures.

3 Résumé

Plusieurs vulnérabilités dans lha permettent à un utilisateur mal intentionné de créer un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

lha est un utilitaire d'archivage et de compression pour les archives au format LHarc. Plusieurs vulnérabilités ont été découvertes :

- Une vulnérabilité de type débordement de mémoire dans le traitement des archives au format LHarc (CAN-2004-0769) ;

– plusieurs vulnérabilités de type débordement de mémoire dans l'analyse des arguments passés en ligne de commande (CAN-2004-0694 et CAN-2004-0771) ;
– une vulnérabilité de type débordement de mémoire dans l'interprétation des noms de répertoire (CAN-2004-0745).

Ces vulnérabilités permettent à un utilisateur mal intentionné, à l'aide d'une archive LHarc, d'un répertoire ou d'une ligne de commande habilement constituée, de créer un déni de service ou d'exécuter du code arbitraire à distance sur la machine victime.

5 Solution

Se référer à la section Documentation pour l'obtention des correctifs.

6 Documentation

– Bulletin de sécurité RedHat RHSA-2004:323 du 01 septembre 2004 :
http://rhn.redhat.com/errata/RHSA-2004-323.html
– Bulletin de sécurité Gentoo GLSA 200409-13 du 08 septembre 2004 :
http://www.gentoo.org/security/en/glsa/glsa-200409-13.xml
– Bulletin de sécurité FreeBSD pour lha du 23 septembre 2004 :
http://www.vuxml.org/freebsd
– Référence CVE CAN-2004-0694 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0694
– Référence CVE CAN-2004-0745 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0745
– Référence CVE CAN-2004-0769 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0769
– Référence CVE CAN-2004-0771 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0771

Gestion détaillée du document

02 septembre 2004 version initiale.
09 septembre 2004 ajout de la référence au bulletin de sécurité Gentoo.
28 septembre 2004 ajout de la référence au bulletin de sécurité FreeBSD.