



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 juin 2004
N° CERTA-2004-AVI-147-005

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de LHA

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-147>

Gestion du document

Référence	CERTA-2004-AVI-147-005
Titre	Vulnérabilité de LHA
Date de la première version	30 avril 2004
Date de la dernière version	09 juin 2004
Source(s)	Avis de sécurité RedHat RHSA-2004:179
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

- Création de fichiers arbitraires ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

Toutes les versions de LHA.

3 Résumé

Plusieurs vulnérabilités dans LHA permettent à un utilisateur mal intentionné de créer des fichiers arbitraires 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 :

- Deux vulnérabilités de type débordement de mémoire (CAN-2004-234) ;

– deux vulnérabilités de type traversée de répertoire (CAN-2004-235).
Ces vulnérabilités permettent à un utilisateur mal intentionné, à l'aide d'une archive LHarc habilement constituée, de créer des fichiers arbitraires 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

- Avis de sécurité RedHat RHSA-2004:178 du 26 mai 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-178.html>
- Avis de sécurité RedHat RHSA-2004:179 du 30 avril 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-179.html>
- Avis de sécurité Gentoo GLSA-200405-02 :
<http://www.gentoo.org/security/en/glsa/glsa-200405-02.xml>
- Avis de sécurité Debian DSA-515 du 05 juin 2004 :
<http://www.debian.org/security/2004/dsa-515>
- Avis de sécurité SUSE SuSE-SA:2004:015 du 09 juin 2004 :
http://www.suse.com/de/security/2004_15_cvs.html
- Avis de sécurité FreeBSD du 02 mai 2004 :
<http://www.vuxml.org/freebsd/>
- Avis de sécurité pour le paquetage OpenBSD lha du 06 mai 2004 :
<http://www.vuxml.org/openbsd/>
- Mise à jour de sécurité pour le paquetage NetBSD lha :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/distfiles/vulnerabilities>
- Référence CVE CAN-2004-0234 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0234>
- Référence CVE CAN-2004-0235 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0235>

Gestion détaillée du document

30 avril 2004 version initiale.

10 mai 2004 ajout de la référence au bulletin de sécurité Gentoo.

12 mai 2004 ajout des références aux bulletins de sécurité FreeBSD, OpenBSD et NetBSD.

08 juin 2004 ajout de la référence au bulletin de sécurité Debian.

09 juin 2004 ajout de la référence au second bulletin de sécurité RedHat.

09 juin 2004 ajout de la référence au bulletin de sécurité SUSE.