Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 6 janvier 2004
N° CERTA-2003-AVI-210-03

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de lftp

Gestion du document

Référence	CERTA-2003-AVI-210-03
Titre	Vulnérabilité de lftp
Date de la première version	16 décembre 2003
Date de la dernière version	6 janvier 2004
Source(s)	Bulletin de sécurité SuSE-SA:2003:051 de SuSE Bulletin de sécurité MDKSA-2003:116 de Mandrake
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

`lftp` versions 2.3.0 à 2.6.9 incluse.

3 Résumé

Une vulnérabilité présente dans `lftp` permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance sur la plate-forme vulnérable.

4 Description

`lftp` est un client permettant le transfert de fichiers depuis des serveurs FTP ou HTTP.

Une vulnérabilité de type débordement de mémoire est présente dans le traitement de la réponse à une commande `ls` ou `rels` émise lors d'une session réalisée avec un serveur WEB au moyen des protocoles HTTP ou HTTPS.

Il est ainsi possible, pour un administrateur mal intentionné, de créer un site WEB avec des répertoires constitués de telle façon que, lors de l'analyse du résultat de la réponse à la commande `ls` ou `rels` renvoyé par le serveur WEB, du code arbitraire soit exécuté sur la plate-forme client vulnérable.

5 Solution

La version 2.6.10 de `lftp` corrige cette vulnérabilité.

6 Documentation

- Site de lftp :
  http://lftp.yar.ru/news.html
- Bulletin de sécurité MDKSA-2003:116 de Mandrake :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:116
- Bulletin de sécurité SuSE-SA:2003:51 de SuSE :
  http://www.suse.com/de/security/2003_051_lftp.html
- Bulletin de sécurité RHSA-2003:403 de RedHat :
  http://rhn.redhat.com/errata/RHSA-2003-403.html
- Bulletin de sécurité RHSA-2003:404 de RedHat :
  http://rhn.redhat.com/errata/RHSA-2003-404.html
- Bulletin de sécurité 200312-07 de Gentoo :
  http://www.securityfocus.com/advisories/6181
- Bulletin de sécurité DSA-406 de Debian :
  http://www.debian.org/security/2004/dsa-406
- Référence CVE CAN-2003-0963 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0963

Gestion détaillée du document

16 décembre 2003 version initiale.

17 décembre 2003 ajout références aux bulletins de sécurité de RedHat.

19 décembre 2003 ajout référence au bulletin de sécurité de Gentoo.

6 janvier 2004 ajout référence au bulletin de sécurité de Debian.