

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de cURL/libcURL

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-2005-AVI-482>

Gestion du document

Référence	CERTA-2005-AVI-482-002
Titre	Vulnérabilité de cURL/libcURL
Date de la première version	08 décembre 2005
Date de la dernière version	21 décembre 2005
Source(s)	Bulletin de sécurité cURL/libcURL du 07 décembre 2005
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

cURL 7.x.

3 Résumé

Une vulnérabilité dans la bibliothèque libcURL permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

La bibliothèque libcURL comporte de nombreuses fonctions permettant le transfert de fichiers en utilisant des syntaxes de type adresses réticulaires (URL).

Une vulnérabilité de type débordement de mémoire, due à une mauvaise gestion des URL dont la longueur est supérieure à 256 octets, peut être exploitée par un utilisateur mal intentionné, au moyen d'une requête HTTP malicieusement constituée, afin d'exécuter du code arbitraire sur la machine vulnérable.

5 Solution

Mettre à jour cURL en version 7.15.1. cURL peut être téléchargé à l'adresse suivante :
<http://curl.haxx.se/download.html>

Dans tous les cas se référer aux bulletins de sécurité des éditeurs pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site Internet de cURL / libcurl :
<http://curl.haxx.se>
- Bulletin de sécurité cURL du 07 décembre 2005 :
http://curl.haxx.se/docs/adv_20051207.html
- Bulletin de sécurité Mandriva MDKSA-2005:224 du 08 décembre 2005 :
<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:224>
- Bulletin de sécurité Debian DSA-919 du 12 décembre 2005 :
<http://www.debian.org/security/2005/dsa-919>
- Bulletin de sécurité FreeBSD pour cURL du 09 décembre 2005 :
<http://www.vuxml.org/freebsd/pkg-curl.html>
- Bulletin de sécurité Gentoo GLSA 200512-09 du 16 décembre 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200512-09.xml>
- Bulletin de sécurité RedHat RHSA-2005:875 du 20 décembre 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-875.html>
- Référence CVE CAN-2005-4077 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-4077>

Gestion détaillée du document

08 décembre 2005 version initiale.

13 décembre 2005 ajout des références aux bulletins de sécurité Debian, Mandriva et FreeBSD et ajout de la référence CVE.

21 décembre 2005 ajout des références aux bulletins de sécurité Gentoo GLSA 200512-09 et RedHat RHSA-2005:875.