

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-2011-AVI-373>

Gestion du document

Référence	CERTA-2011-AVI-373
Titre	Vulnérabilité dans libcurl
Date de la première version	29 juin 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité cURL du 23 juin 2011
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

Atteinte à la confidentialité des données.

2 Systèmes affectés

libcurl versions 7.10.6 à 7.21.6 incluses.

3 Résumé

Une vulnérabilité dans libcurl permet à un serveur malveillant de se faire passer pour le client auprès d'autres entités utilisant les mécanismes GSSAPI.

4 Description

Lors d'une authentification GSSAPI, libcurl fournit au serveur une copie des justificatifs d'identité du client. Le serveur peut alors utiliser ceux-ci pour se faire passer pour le client auprès d'autres entités.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité cURL du 23 juin 2011 :
http://curl.haxx.se/docs/adv_20110623.html
- Référence CVE CVE-2011-2192 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2192>

Gestion détaillée du document

29 juin 2011 version initiale.