

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans 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-2013-AVI-107>

---

### Gestion du document

Référence	CERTA-2013-AVI-107
Titre	Vulnérabilité dans cURL libcurl
Date de la première version	08 février 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité cURL du 06 février 2013
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(s)

– exécution de code arbitraire à distance

## 2 Systèmes affectés

cURL de la version 7.26.0 à la 7.28.1

## 3 Résumé

Une vulnérabilité a été corrigée dans *cURL libcurl*. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance au moyen d'un serveur SMTP, POP3 ou IMAP spécialement conçu.

## 4 Solution

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

## **5 Documentation**

- Bulletin de sécurité cURL du 06 février 2013  
[http://curl.haxx.se/docs/adv\\_20130206.html](http://curl.haxx.se/docs/adv_20130206.html)
- Référence CVE CVE-2013-0249  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0249>

### **Gestion détaillée du document**

**08 février 2013** version initiale.