

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans cURL

---

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-2009-AVI-105>

---

### Gestion du document

Référence	CERTA-2009-AVI-105
Titre	Vulnérabilité dans cURL
Date de la première version	18 mars 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité cURL du 03 mars 2009
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 ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

- cURL et libcurl versions antérieures à 7.19.4.

## 3 Résumé

Une vulnérabilité de *cURL* et de *libcurl* permet à un individu distant d'exécuter du code arbitraire ou de contourner la politique de sécurité.

## 4 Description

Une vulnérabilité présente dans l'implémentation de la fonction *redirect* (la fonctionnalité de suivre les redirections) de *cURL* et de *libcurl* permet à un individu distant de contourner la politique de sécurité. Les versions de *cURL* et de *libcurl* compilées pour prendre en charge SCP permettent également à un individu distant d'exécuter du code arbitraire à distance par le biais d'une redirection utilisant le caractère « ; » de façon particulière.

## **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 03 mars 2009 :  
[http://curl.haxx.se/docs/adv\\_20090303.html](http://curl.haxx.se/docs/adv_20090303.html)
- Référence CVE CVE-2009-0037 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0037>

## **Gestion détaillée du document**

**18 mars 2009** version initiale.