

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de cURL et 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-2009-AVI-338>

---

### Gestion du document

Référence	CERTA-2009-AVI-338-002
Titre	Vulnérabilité de cURL et libcurl
Date de la première version	17 août 2009
Date de la dernière version	21 août 2009
Source(s)	Bulletin de sécurité du projet cURL du 12 août 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

Contournement de la politique de sécurité.

## 2 Systèmes affectés

cURL et libcurl, jusqu'à la version 7.19.5.

## 3 Résumé

Une vulnérabilité dans cURL et libcurl permet à un utilisateur malveillant de contourner la politique de sécurité.

## 4 Description

Une vulnérabilité est présente dans cURL et libcurl qui, quand OpenSSL est utilisé, permet à un utilisateur malveillant de tromper l'utilisateur sur l'identité du serveur auquel il est connecté.

## 5 Solution

La version 7.19.6 remédie à cette vulnérabilité. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité du projet cURL du 12 août 2009 :  
[http://curl.haxx.se/docs/adv\\_20090812.txt](http://curl.haxx.se/docs/adv_20090812.txt)
- Bulletin de sécurité Debian DSA-1869-1 du 19 août 2009 :  
<http://www.debian.org/security/2009/dsa-1869>
- Bulletin de sécurité Mandriva MDVSA-2009:203 du 15 août 2009 :  
<http://www.mandriva.com/en/security/advisories?name=MDVSA-2009:203>
- Bulletin de sécurité RedHat RHSA-2009:1209-1 du 13 août 2009 :  
<http://rhn.redhat.com/errata/RHSA-2009-1209-1.html>
- Bulletin de sécurité Ubuntu USN-818-1 du 17 août 2009 :  
<http://www.ubuntu.com/usn/usn-818-1>
- Référence CVE CVE-2009-2417 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2417>
- Référence CVE CVE-2009-2408 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2408>

## Gestion détaillée du document

**17 août 2009** version initiale.

**19 août 2009** ajout des références aux bulletins RedHat et Ubuntu.

**21 août 2009** ajout des références aux bulletins Mandriva et Debian.