



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

**S . G . D . S . N**  
Agence nationale de la sécurité  
des systèmes d'information  
CERTA

Paris, le 22 mars 2006  
N° CERTA-2006-AVI-116-002

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-2006-AVI-116>

---

### Gestion du document

Référence	CERTA-2006-AVI-116-002
Titre	Vulnérabilité dans cURL
Date de la première version	20 mars 2006
Date de la dernière version	22 mars 2006
Source(s)	Liste des changements apportés à la version 7.15.3
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 versions 7.15.2 et antérieures.

## 3 Résumé

Une vulnérabilité dans cURL permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire.

## 4 Description

Une vulnérabilité de type débordement de tampon dans la mise en œuvre du protocole TFTP par cURL permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire par le biais d'une URL malicieusement construite.

## 5 Solution

La version 7.5.13 de cURL corrige le problème :  
<http://curl.haxx.se/download.html>

## 6 Documentation

- Site de cURL :  
<http://curl.haxx.se>
- Liste des changements apportés à la version 7.15.3 de cURL :  
<http://curl.haxx.se/changes.html>
- Bulletin de sécurité FreeBSD pour curl du 20 mars 2006 :  
<http://www.vuxml.org/freebsd/pkg-curl.html>
- Bulletin de sécurité Gentoo GLSA 200603-19 du 21 mars 2006 :  
<http://www.gentoo.org/security/en/glsa/glsa-200603-19.xml>
- Référence CVE CVE-2006-1061 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1061>

## Gestion détaillée du document

**20 mars 2006** version initiale.

**21 mars 2006** ajout de la référence au bulletin de sécurité FreeBSD.

**22 mars 2006** ajout de la référence au bulletin de sécurité Gentoo.