

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités 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-2005-AVI-093>

---

### Gestion du document

Référence	CERTA-2005-AVI-093-002
Titre	Vulnérabilités dans cURL/libcURL
Date de la première version	01 mars 2005
Date de la dernière version	17 mars 2005
Source(s)	Bulletins de sécurité iDefense du 21 février 2005
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 7.12.1 et antérieures.

## 3 Résumé

Deux vulnérabilités dans cURL/libcURL permettent l'exécution de code arbitraire à distance.

## 4 Description

cURL est un outil en ligne de commande permettant de transférer des fichiers.

Une première vulnérabilité de type débordement de mémoire existe dans l'authentification NTLM (NT Lan Manager).

Une seconde vulnérabilité de type débordement de mémoire existe dans l'authentification Kerberos.

Un utilisateur mal intentionné peut, en incitant sa victime à se connecter à un serveur malicieux en utilisant l'authentification NTLM ou l'authentification Kerberos, exécuter du code arbitraire à distance.

## 5 Solution

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

## 6 Documentation

- Site de cURL :  
<http://cool.haxx.se/curl/>
- Bulletin de sécurité de FreeBSD du 27 février 2005 :  
<http://www.vuxml.org/freebsd/pkg-curl.html>
- Bulletin de sécurité de NetBSD :  
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/www/curl/README.html>
- Bulletin de sécurité SUSE SUSE-SA:2005:011 :  
[http://www.novell.com/linux/security/advisories/2005\\_11\\_curl.html](http://www.novell.com/linux/security/advisories/2005_11_curl.html)
- Bulletin de sécurité Mandrake MDKSA-2005:048 du 04 mars 2005 :  
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:048>
- Bulletin de sécurité Gentoo GLSA 200503-20 du 16 mars 2005 :  
<http://www.gentoo.org/security/en/glsa/glsa-200503-20.xml>
- Référence CVE CAN-2005-0490 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0490>

## Gestion détaillée du document

**01 mars 2005** version initiale.

**07 mars 2005** ajout de la référence au bulletin de sécurité Mandrake.

**17 mars 2005** ajout de la référence au bulletin de sécurité Gentoo.