

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans glibc

---

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-2010-AVI-520>

---

### Gestion du document

|                             |   |
|-----------------------------|---|
| Référence                   | CERTA-2010-AVI-520                        |
| Titre                       | Vulnérabilité dans glibc                  |
| Date de la première version | 28 octobre 2010                           |
| Date de la dernière version | –   |
| Source(s)                   | Avis de sécurité Red Hat RHSA-2010:0787-1 |
| 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

Élévation de privilèges.

## 2 Systèmes affectés

GNU glibc 2.x

## 3 Résumé

Une vulnérabilité dans la bibliothèque `glibc` permet à un utilisateur malintentionné d'élever ses privilèges.

## 4 Description

Une vulnérabilité a été corrigée dans l'éditeur de liens de `glibc`. Ce dernier ne contrôle pas correctement le champ `$ORIGIN` dans la variable d'environnement `LD_AUDIT`. Un attaquant local, avec les droits d'accès en écriture sur un système contenant des exécutable avec les attributs `setuid` ou `setgid` activés, peut utiliser cette vulnérabilité pour élever ses privilèges.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité RedHat RHSA-2010:0787 du 20 octobre 2010 :  
<http://rhn.redhat.com/errata/RHSA-2010-0787.html>
- Référence CVE CVE-2010-3847 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3847>

## **Gestion détaillée du document**

**28 octobre 2010** version initiale.