



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 23 mai 2006  
N° CERTA-2006-AVI-214

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de GNU Binutils

---

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-214>

---

### Gestion du document

Référence	CERTA-2006-AVI-214
Titre	Vulnérabilité de GNU Binutils
Date de la première version	23 mai 2006
Date de la dernière version	–
Source(s)	
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 ;
- déni de service.

## 2 Systèmes affectés

La version de GNU Binutils 2.16.1 ainsi que celles antérieures.

## 3 Résumé

Une vulnérabilité dans GNU Binutils peut permettre à un utilisateur malveillant de créer un déni de service ou d'exécuter des commandes arbitraires sur le système vulnérable.

## 4 Description

GNU Binutils est un groupe d'outils fourni dans la plupart des distributions Linux, et permettant de travailler sur des fichiers au format binaire : parmi eux se trouvent `strings` (pour lister les chaînes de caractères incluses dans

le code binaire), `ld` (ou *GNU Linker* pour terminer une compilation), l'assembleur `as`, etc. Ces outils emploient un ensemble commun de bibliothèques.

Une vulnérabilité a été identifiée dans l'une d'entre elles, `libbfd` : elle ne gère pas correctement, quand un fichier contient une entrée au format Tektronix Hex (TekHex), une valeur dont la longueur ne correspond pas à un caractère hexadécimal. Un utilisateur malveillant peut donc construire un fichier particulier pour créer un débordement de tampon. Ce dernier peut provoquer un déni de service ou l'exécution de commandes arbitraires dans le cas où une personne le manipule avec l'un des outils GNU Binutils.

## 5 Solution

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

## 6 Documentation

- Référence CVE CVE-2006-2362 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2362>
- Site du projet GNU Binutils :  
<http://www.gnu.org/software/binutils/>
- Référence du bogue et correctif provisoire :  
[http://sourceware.org/bugzilla/show\\_bug.cgi?id=2584](http://sourceware.org/bugzilla/show_bug.cgi?id=2584)

## Gestion détaillée du document

**23 mai 2006** version initiale.