

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités de Common Data Format

---

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-288>

---

### Gestion du document

Référence	CERTA-2009-AVI-288
Titre	Multiples vulnérabilités de Common Data Format
Date de la première version	24 juillet 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité sur CDF de la NASA
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 ;
- déni de service à distance.

## 2 Systèmes affectés

CDF versions 3.2.4 et antérieures.

## 3 Résumé

Plusieurs vulnérabilités présentes dans le produit Common Data Format (CDF) permettent à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire.

## 4 Description

Common Data Format (CDF) est un logiciel en sources ouvertes fourni par la NASA pour manipuler les fichiers au format homonyme. CDF peut être utilisé avec des logiciels comme MatLab pour des opérations particulières.

Deux vulnérabilités sont présentes dans le logiciel CDF. Elles sont relatives à plusieurs fonctions comme *ReadAEDRList64()*, *SearchForRecord\_r\_64()*, *LastRecord64()* ou *CDFsel64()*. Ces failles permettent à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire via un fichier CDF particulier.

## 5 Solution

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

La version 3.3 de CDF corrige le problème :

`ftp://cdaweb.gsfc.nasa.gov/pub/cdf/dist/latest-release2`

## 6 Documentation

- Site de CDF :  
<http://cdf.gsfc.nasa.gov>
- Bulletin de sécurité sur CDF de la NASA :  
[http://cdf.gsfc.nasa.gov/html/CDF\\_v330.html](http://cdf.gsfc.nasa.gov/html/CDF_v330.html)

## Gestion détaillée du document

24 juillet 2009 version initiale.