



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 03 avril 2007  
N° CERTA-2007-AVI-152

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans ImageMagick

---

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-2007-AVI-152>

---

### Gestion du document

Référence	CERTA-2007-AVI-152
Titre	Multiples vulnérabilités dans ImageMagick
Date de la première version	03 avril 2007
Date de la dernière version	–
Source(s)	Liste des changements apportés à la version 6.3.3-5 de ImageMagick
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.

## 2 Systèmes affectés

ImageMagick versions 6.3.3-3 et antérieures.

## 3 Résumé

De multiples vulnérabilités dans ImageMagick permettent à un utilisateur d'exécuter du code arbitraire sur la machine vulnérable.

## 4 Description

ImageMagick est un ensemble d'outils permettant la manipulation de divers formats d'images. Trois vulnérabilités de type débordement de mémoire y ont été identifiées :

- la première concerne la mise en œuvre du support des images au format DCM ;
- les deux autres se rapportent à la gestion des images au format XWD.

Ces vulnérabilités peuvent être exploitées par le biais d'images spécialement conçues et permettent d'exécuter du code arbitraire.

## **5 Solution**

La version 6.3.3-5 de ImageMagick corrige le problème :

<http://www.imagemagick.org/script/download.php>

## **6 Documentation**

- Site de ImageMagick :  
<http://www.imagemagick.org>
- Liste des changements apportés à la version 6.3.3-5 de ImageMagick :  
<http://www.imagemagick.org/script/changelog.php>
- Référence CVE CVE-2007-1797 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1797>

## **Gestion détaillée du document**

**03 avril 2007** version initiale.