



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 septembre 2007
N° CERTA-2007-AVI-414

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-414>

Gestion du document

Référence	CERTA-2007-AVI-414
Titre	Multiples vulnérabilités dans ImageMagick
Date de la première version	24 septembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Secunia 26926 du 24 septembre 2007
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.

Exécution de code arbitraire.

2 Systèmes affectés

Les versions antérieures à la 6.3.5-10.

3 Résumé

De multiples vulnérabilités dans ImageMagick permettent à un utilisateur de provoquer des dénis de service ou d'exécuter du code arbitraire à distance sur la machine vulnérable.

4 Description

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

5 Solution

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

6 Documentation

- Liste des changements apportés à la version 6.3.5-10 de ImageMagick :
<http://www.imagemagick.org/script/changelog.php>
- Bulletin de sécurité Secunia 26926 du 04 septembre du 2007 :
<http://secunia.com/advisories/26926/>
- Référence CVE CVE-2007-4986 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4986>
- Référence CVE CVE-2007-4987 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4987>
- Référence CVE CVE-2007-4988 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4988>

Gestion détaillée du document

24 septembre 2007 version initiale.