

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-2005-AVI-179>

Gestion du document

Référence	CERTA-2005-AVI-179
Titre	Vulnérabilité de ImageMagick
Date de la première version	27 mai 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Damian Put du 25 avril 2005
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

- Déni de service ;
- exécution de code arbitraire.

2 Systèmes affectés

Toutes les versions de ImageMagick antérieures à la version 6.2.2.

3 Description

ImageMagick est un ensemble d'outils destinés au traitement d'images. Une vulnérabilité de type débordement de mémoire présente dans le traitement des images au format PNM peut être exploitée par une personne mal intentionnée en mettant à disposition de l'utilisateur d'ImageMagick une image habilement constituée.

4 Solution

La version 6.2.2 de ImageMagick corrige ces vulnérabilités. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Site Internet de ImageMagick :
<http://www.imagemagick.org>
- Liste des changements de ImageMagick :
<http://www.imagemagick.org/script/changelog.php>
- Bulletin de sécurité de Damian Put du 25 avril 2005 :
<http://www.overflow.pl/adv/imheapoverflow.txt>
- Bulletin de sécurité RedHat RHSA-2005-413 du 25 mai 2005 :
<https://rhn.redhat.com/errata/RHSA-2005-413.html>
- Référence CVE CAN-2005-1275 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1275>

Gestion détaillée du document

27 mai 2005 version initiale.